IBM Optim

Installation and Configuration Guide

Version 7.0 Release 1

IBM Optim

Installation and Configuration Guide

Version 7.0 Release 1

Note:
Before using this information and the product it supports, read the information on the next page.

This edition applies to Version 7, Release 1 of IBM Optim and to all subsequent releases and modifications until otherwise indicated in new editions.

© IBM Corporation, 1998-2008

IBM Optim
Installation and Configuration Guide

This manual and the software described in it are furnished under a license agreement or nondisclosure agreement. The software and the documentation may be used only in accordance with the terms of that agreement. No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose without the express written permission of IBM Corporation.

IBM Optim Installation and Configuration Guide,
Version 7.0 Release 1, November 2008

Trademark Acknowledgments

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Intel and Pentium are registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Contents

About this Guide xiii
Summary of Release 7.1 xvii
Summary of Release 6.5 xix
Summary of Release 6.4 xxii
1. Getting Started 1
1.1 Conceptual Overview 1
1.1.1 Installation Phase 4
1.1.2 Configuration Phase 6
1.2 Planning for Installation and Configuration 10
1.2.1 Installation Requirements 11
1.2.2 Required Database Permissions 14
1.2.3 Required Server Authorizations 19
1.2.4 Character Formats 21
1.3 Troubleshooting Your Installation 30
1.3.1 Image Locator Diagnostic Tool 30
1.3.2 Oracle Connection Diagnostic Tool 31
1.3.3 Microsoft Debugging Utility 32
2. Installation Setup 35
2.1 Run Setup 37
2.1.1 Software License 38
2.1.2 Customer Information 39
2.1.3 Select the Type of Setup 40
2.1.4 Choose Destination Location 41
2.1.5 Select Components 42
2.1.6 Select Program Folder 44
2.1.7 Start Copying Files 45
2.1.8 Installation 45
2.2 Installation Complete 46
2.3 Configuration Overview 47
3. Signing an Optim Exit 49
3.1 Writing Your Own Exit 51
3.2 Prerequisites to Signing a User-Supplied Exit 52
3.3 Signing an Exit in Windows 53

3.4 Changing a Signed Optim Exit 55
3.5 The Sign Optim Exit Dialog 56
3.6 Specifying a Company Name and ID 60
4. Configuration Window and Menus 61
4.1 Main Window and Menus 62
4.1.1 Main Window 62
4.1.2 Menus 63
4.1.3 Processing Log 70
4.1.4 Configuration Assistant 71
4.1.5 Dialogs 73
5. Configure Workstations 77
5.1 Configure the First Workstation 78
5.1.1 Specify Product License Key 78
5.1.2 Create Optim Directory 78
5.1.3 Create DB Aliases 94
5.1.4 Optim Security 128
5.1.5 Configure Options 132
5.1.6 Export Registry Data 137
5.1.7 Summary 139
5.2 Configure Additional Workstation 140
5.2.1 Import Registry Entries 141
5.2.2 Create Registry Entry 143
5.2.3 Initialize Security/Change Security Administrator 147
5.2.4 Enable/Disable Optim Server Feature 148
5.2.5 Enable/Disable Archive ODBC Interface 149
5.2.6 Specify Product Configuration File 149
5.2.7 Summary 150
6. Configure the Optim Server 151
6.1 General Tab 154
6.2 Errors Tab 156
6.3 Load Tab 158
6.4 Connection Tab 160
6.5 Access Tab 163
6.6 Startup Tab 164
6.7 Security Tab 166
6.8 Endpoints Tab 169
6.9 Archive Tab 173
6.10 Retention Tab 175
6.11 Status Tab 177
6.12 Email Tab 179
6.13 Conclusion 182
7. Maintenance and Other Configuration Tasks 183
7.1 Create/Update DB Alias 185
7.2 Create/Update Optim Directory 190
7.3 Access Existing Optim Directory 191

7.4 Configure Security for an Optim Directory 192
7.4.1 Specify Optim Directory 192
7.4.2 Initialize Security or Change Security Administrator 193
7.4.3 Set Functional Security Option 196
7.4.4 Set Optim Object Security Option 197
7.4.5 Set Archive File Security Option 200
7.5 Enable/Disable this Machine as an Optim Server 201
7.6 Enable/Disable the ODBC Interface for this Machine 202
7.7 Apply Maintenance for Optim Directory Access 203
7.8 Apply Maintenance for DB Alias Access 205
7.8.1 Query Method to Apply Maintenance? 206
7.8.2 Apply Maintenance for a Single DB Alias 207
7.8.3 Apply Maintenance for All DB Aliases 209
7.8.4 Apply Maintenance for Specific DBMS 210
7.9 Rename an Optim Directory 213
7.9.1 Rename an Optim Directory and the Windows Registry Entry 215
7.9.2 Only Rename the Windows Registry Entry 219
7.10 Update DBMS Version for an Optim Directory 221
7.11 Update DBMS Version for a DB Alias 224
7.11.1 Update DBMS for a Single DB Alias 224
7.11.2 Update Multiple DB Aliases 228
7.12 Configure Options 232
7.13 Create Primary Keys 233
7.14 Create Copies of DB2 z/OS Relationships 235
7.15 Load/Drop Sample Data 236
7.16 Load/Drop Data Privacy Data 237
7.17 Drop DB Alias or Optim Tables 238
7.17.1 Drop the Optim Directory? 242
7.18 Purge Optim Directory Registry Entry 243
7.19 Purge DB Alias 244
8. Product Options 245
8.1 Open the Product Options Editor 246
8.2 Using the Editor 248
8.2.1 General Tab 249
8.2.2 Database Tab 252
8.2.3 Configuration File Tab 257
8.2.4 Password Tab 258
8.2.5 Edit Tab 259
8.2.6 Servers Tab 268
8.2.7 Archive Tab 270
8.2.8 Load Tab 274
8.2.9 Report Tab 276
9. Personal Options 279
9.1 Open the Personal Options Editor 280
9.2 Using the Editor 282

9.2.1 General Tab 284
9.2.2 Confirm Tab 286
9.2.3 Display Tab 287
9.2.4 Errors Tab 290
9.2.5 Scheduling Tab 292
9.2.6 Load Tab 293
9.2.7 Create Tab 294
9.2.8 Logon Tab 303
9.2.9 Server Tab 305
9.2.10 Edit Tab 308
9.2.11 Browse Tab 313
9.2.12 Archive Tab 315
9.2.13 Removable Media Tab 317
9.2.14 Actions Tab 318
9.2.15 Printer Tab 324
9.2.16 Database Tab 326
9.2.17 Notify Tab 330
Appendix A. Install and Configure the Server under UNIX or Linux 333
A.1 Installation 335
A.1.1 Run Setup 335
A.1.2 Command Line Installation 351
A.2 Configuration 358
A.2.1 Pstserv Configuration File 360
A.2.2 Pstlocal Configuration File for the Command Line Utility 370
A.2.3 RTSETENV Shell Script 386
A.2.4 RTSERVER Shell Script 387
A.2.5 RT4S Shell Script 389
A.2.6 LOCALE.CONF Conversion File 390
A.3 Maintenance and Performance 391
A.3.1 Commands 391
A.3.2 Temporary Files 393
A.4 Securing the Products and Configuration Files 394
A.4.1 Securing the Products 394
A.4.2 Securing the Configuration Files 398
A.5 The Optim Exit in UNIX 403
A.5.1 Writing Your Own Exit 405
A.5.2 Prerequisites to Signing a User-Supplied Exit 405
A.5.3 Signing an Exit in UNIX 406
A.5.4 The Invalid Credentials Specified Dialog 407
A.5.5 The Sign Optim Exit Failed Dialog 408
A.5.6 Signing the Default Exit after an Installation 409
A.5.7 Signing a User-Supplied Exit in UNIX 413
Appendix B. Server Credentials 417
B.1 Server Credentials 418
B.1.1 Credentials to Run the Server 418

B.1.2 Credentials to Run Optim Processes 419
B.1.3 Server Privileges for Explicit or Client Credentials 422
B.1.4 UNC Network Share Access (Windows) 422
B.1.5 Registry Access for Process Requests (Windows) 423
B.1.6 Oracle OS Authentication 424
B.1.7 UNIX or Linux File Access 424
B.2 DBMS Logon Credentials 425
Appendix C. Command Line Maintenance Tasks 429
C.1 Syntax and Keywords 431
C.2 Examples 438
C.2.1 Create Multiple DB Aliases with one Optim Directory 438
C.2.2 Apply Maintenance to Multiple DB Aliases 439
Appendix D. Optim Security 441
D.1 Access Control Domain 447
D.1.1 Access Control Domain Editor 450
D.1.2 Role Specifications 452
D.1.3 Users Tab 454
D.1.4 Privileges Tabs 457
D.2 Access Control List 469
D.2.1 Access Control List Editor 471
D.3 File Access Definition 478
D.3.1 File Access Definition Editor 480
D.3.2 Defining Access Permissions for Columns 486
D.3.3 File Access Definition Example 492
D.4 Exporting Security Definitions 496
D.5 Import Security Definitions 500
D.5.1 Import Dialog 500
Appendix E. Security Reports 511
E.1 Open the Report Request Editor 513
E.1.1 Create a New Report Request 513
E.1.2 Select a Report Request to Edit 514
E.2 Using the Editor 515
E.2.1 General Tab 517
E.2.2 Security Criteria 518
E.2.3 Notify Tab 522
E.3 Process a Report Request 523
E.3.1 Schedule a Report Process 523
E.3.2 Run a Report Request 523
E.3.3 Report Process Report 524
Appendix F. Open Data Manager 527
F.1 Installation 528
F.1.1 Windows Installation 528
F.1.2 UNIX Installation 531
F.1.3 UNIX Administration 533
F.1.4 Attunity Studio Configuration 534

F.2 Define the ODM Data Source on the Primary Server 538
F.3 Secondary Server Configuration 542
F.4 Thin Client Installation 547
F.4.1 ODBC Thin Client 547
F.4.2 JDBC Thin Client 547
F.5 ODM Security 548
F.6 Runtime Connection Information 554
F.7 ODM Data Type Conversions 556
F.8 Archive File to XML Convertor 557
F.9 Archive File Collections 561
F.9.1 Archive File Collection Subsets 562
F.9.2 PST_ARCHIVE_ID Pseudocolumn 563
F.9.3 PST_ARCHIVE_FILES Table 563
Appendix G. Converting PST and Optim Directory Objects 565
G.1 Conversion Process for 5.x Optim Directories 567
G.1.1 Step 1: Create a New Optim Directory 568
G.1.2 Step 2: Export Data from Old Optim Directory 571
G.1.3 Step 3: Import Data into New Optim Directory 577
G.2 Conversion Process for Directory Tables on SQL Server 583
G.2.1 Converting Version 6.0/6.1 Directory Tables in SQL Server . 583
G.2.2 Dropping Version 6.0/6.1 Directory Tables 584
Appendix H. Samples 587
H.1 Sample Database Tables and Structure 588
H.1.1 OPTIM_SALES Table 590
H.1.2 OPTIM_CUSTOMERS Table 591
H.1.3 OPTIM_ORDERS Table 593
H.1.4 OPTIM_DETAILS Table 594
H.1.5 OPTIM_ITEMS Table 595
H.1.6 OPTIM_SHIP_TO Table 596
H.1.7 OPTIM_SHIP_ INSTR Table 597
H.1.8 OPTIM_MALE_RATES Table 597
H.1.9 OPTIM_FEMALE_RATES Table 598
H.1.10 OPTIM_STATE_LOOKUP Table 598
H.2 Sample Column Map Exits 599
H.3 Sample Column Map Procedures 601
H.4 Sample Extract Files 603
H.5 Sample JCL File 603
Appendix I. Data Privacy Data Tables 605
I.1 Content of Data Privacy Tables 606
Appendix J. Uninstalling 611
J.1 Prompt Before Dropping Each Set of Optim Database Objects 613
J.2 Drop All Optim Created Database Objects Without Prompting 613
J.3 Do Not Drop Any Optim Created Database Objects 614
J.4 Cancel the Uninstall Process 614
Index 615

About this Guide

This guide provides information needed to install and configure the IBM® ***Optim***™ solution. This release runs in the Microsoft® Windows® environment, or in the Sun Solaris, Hewlett-Packard HP-UX, IBM AIX®, or Red Hat Linux® environments supplemented with a Windows workstation. ***Optim*** supports the IBM DB2®, Oracle, Sybase Adaptive Server Enterprise (ASE), Microsoft SQL Server, and IBM Informix® database management systems.

The information in this guide is organized into the following chapters.

1. Getting Started	General information about installing and configuring ***Optim*** with suggestions for preparing your site and requirements for hardware, operating systems, and supported database management systems.
2. Installation Setup	Using **Setup** to install ***Optim***.
3. Signing an Optim Exit	Signing the default exit supplied with ***Optim*** or a user-defined exit. Information on writing a user exit to provide additional security for ***Optim*** processes.
4. Configuration Window and Menus	Describes the main window for the **Configuration** program and certain general configuration functions.
5. Configure Workstations	Use these **Configuration** tasks to prepare your system for ***Optim***.

6. Configure the Optim Server	Configure the ***Optim Server*** on one or more Windows workstations.
7. Maintenance and Other Configuration Tasks	After you configure the first and any additional workstations, you are ready to start using ***Optim***. However, it may be necessary to perform other tasks that are available from the **Tasks** menu. You can create, update, or drop DB Aliases and ***Optim*** Directories, Configure Security, enable or disable the ***Optim Server*** or ODBC interface, apply maintenance, update the DBMS version, upgrade ***Optim*** software, configure options, create primary keys, copy IBM DB2 z/OS® relationships, load or drop sample data, and load or drop data privacy data tables (if you have an ***Optim*** Data Privacy License).
8. Product Options	Customize ***Optim*** for all users. You can set general limits for editing and extracting rows of data, specify database options for commit frequency and locking tables, identify the Product Configuration File, and define the password to access Product Options.
9. Personal Options	Personal use customization of ***Optim*** for each workstation. You can customize confirmation prompts, display features, and message text, specify database logon and password information, set defaults for the schedule, browse, and create utilities, and establish default preferences for browsing and editing database tables.

Appendix A. Install and Configure the Server under UNIX or Linux	Prepare your system to use the ***Optim Server*** on a Sun Solaris server, under SPARC; Hewlett-Packard HP-UX server, IBM AIX server, or a Red Hat Application Server, under Linux and modify the corresponding configuration files and shell scripts.
Appendix B. Server Credentials	Credentials used with the ***Optim Server***.
Appendix C. Command Line Maintenance Tasks	Perform certain configuration tasks while bypassing the graphical user interface for ***Optim***.
Appendix D. Optim Security	The three types of ***Optim*** Security — Functional Security, Object Security, and Archive File Security, as well as the security definitions, i.e., Access Control Domains (ACDs), Access Control Lists (ACLs), and File Access Definitions (FADs) used to establish ***Optim*** Security.
Appendix E. Security Reports	Create a report on the permissions for Functional or Object Security privileges assigned to user and group accounts in your network.
Appendix F. Open Data Manager	Provides access to data in ***Optim*** Archive Files for programs that use the ODBC and JDBC APIs.
Appendix G. Converting PST and Optim Directory Objects	Contains information on converting PST Directory objects created in earlier versions of ***Optim*** into a format suitable for use in version 6.0 or later.

Appendix H. Samples	Contains information on the sample database tables, Column Map Exit Routines, Column Map Procedures, Extract Files, and ODBC applications included on the installation CD.
Appendix I. Data Privacy Data Tables	Contains information on the data privacy data data tables included on the installation CD.
Appendix J. Uninstalling	Contains information on using the uninstall procedure for ***Optim***.

Summary of Release 7.1

The following enhancements have been made for release 7.1 of ***Optim***.

Optim

Functionality Enhancements

- **Data Privacy**
  - ***Optim*** data privacy capabilities generate and propagate valid masked values appropriate for application testing. This release includes a new parameter, SEED, in the HASH_LOOKUP function. Use SEED to vary the calculation performed by the hashing algorithm. The hashed value of the source column and the SEED value are matched with a sequential number from the lookup table to obtain the replacement value for the destination column. You may specify a value from 1 to 2,000,000,000.
  - Data privacy transformation library functions allow you to mask personal data such as social security numbers, credit card numbers, and e-mail addresses. The DECIMAL data type is now permitted for source and destination columns for the SSN and CCN functions.
  - Additional lookup tables are included in this release. The tables provide comprehensive data for the following countries: Australia, Canada, Germany, Spain, France, Italy, the UK, and the US.
- **Sample database tables**
  - The prefix OPTIM_ has been added to table names in the sample database.
  - The columns CCN and EMAIL have been added to the OPTIM_CUSTOMERS table.
  - The columns SSN, EMAIL, and PHONE_NUMBER have been added to the OPTIM_SALES table.
  - The column SALESMAN_NAME in the OPTIM_SALES table has been split into the following columns: FIRST_NAME and LAST_NAME.
  - The total number of rows in each table (except for OPTIM_STATE_LOOKUP) has increased.

- **Additional multi-byte code page support**

  For sites using DB2 in the Linux, UNIX, and Windows environments, ***Optim*** now supports additional multi-byte code pages for the Chinese and Korean languages.

Summary of Release 6.5

The following enhancements have been made for release 6.5 of ***Optim***.

Optim

Functionality Enhancements

- **Signed exit for initialization and termination processing**

  Beginning with ***Optim*** release 6.5, an electronically "signed" exit is required to use ***Optim***, whether the exit is the ***Optim*** default exit or a user-supplied exit. To sign an exit, you must enter the "company credentials" supplied to your organization when you received ***Optim***. Your company credentials consist of a supplied company ID, Name, and Password. The ***Optim*** setup process will automatically request these credentials during installation, so you can sign an exit.

  The ***Optim*** default exit is shipped with ***Optim*** and allows all requests by all users, within the security limitations defined for each user or user group using the security functionality included in ***Optim***.

  In addition, ***Optim*** introduces exit points that allow your custom exits to monitor and control the use of ***Optim***. Benefits include data protection, information collection for auditing the use of ***Optim***, and adherence to government regulations. When information is passed to a user-written exit, the exit can allow or disallow the ***Optim*** function.

- **Performance Enhancements**
  - You can route generated process reports to a .TXT file. The file will open automatically at the end of processing using an application such as Notepad.
  - Buffersize options allow you to set the buffer size to use when fetching or deleting rows from the database. ***Optim*** multiplies the buffersize specification by the value set for maximum database connections. You can select a value from 64K to 1024K, in increments of 32. It is recommended that you use the default value unless you are processing tables larger than 10,000 rows.
  - To help you monitor performance, Archive, Extract, and Delete Statistics Reports indicate whether file compression is set on your operating system for the directory used to store process files.

- **Archive File Maintenance Facility**

  The Archive File Maintenance Facility is a command-line driven utility that selectively deletes rows from ***Optim*** Archive Files while maintaining referential integrity within the file. The command to perform Archive File Maintenance is **/AFMF**. Specify the selection criteria identifying the rows to be removed in a command file. The **/AFMF** command can be run only in a Windows environment.

  This feature may help your site adhere to government regulations. You may have to satisfy a requirement, for example, that all records of deceased persons be deleted from storage.

- **Data Privacy**

  Optim data privacy capabilities generate and propagate valid masked values appropriate for application testing. This release includes a new parameter, TRIM, in the HASH_LOOKUP function. Use TRIM to specify a list of characters to be trimmed from the source value or to convert the source value to uppercase, before it is hashed. This parameter helps ensure that certain characters are eliminated so essentially equivalent values will result in HASH_LOOKUP resolving to the same lookup table row. For example, if you choose to trim commas from the source value, the values Smith, John and Smith John will each be hashed to the same value.

  For example, you might specify the following before hashing:

  TRIM=(-) to remove hyphens.

  TRIM=(-) to remove spaces and hyphens.

  TRIM=(\u) to convert source value to uppercase.

  TRIM=(-\u) to remove spaces and hyphens, and convert source value to uppercase.

  TRIM=(\)\\) to remove right parentheses and backslashes.

- **Option to allow Optim Relationships on views**

  You can now define ***Optim*** primary keys and relationships for database views.

Support for DBMS Versions

Optim supports the leading database management systems (Oracle, IBM DB2 z/OS and DB2 LUW, Sybase Adaptive Server Enterprise (ASE), Microsoft SQL Server and IBM Informix).

Optim 6.5 introduces toleration support for the following new releases of databases:

- Informix 11
- DB2 z/OS 9.1
- DB2 LUW 9.5
- Support for XML columns in Oracle 10g and later (carried as LOB)

Summary of Release 6.4

The following enhancements have been made for release 6.4 of ***Optim***.

- **Long Object Name support**

  Archive Files created on ***Optim* z/OS Solution,** a platform that supports long named objects, can be used with ***Optim*** on distributed systems. If an object in the file has a name that exceeds the ***Optim*** maximum, the name is truncated and displays suffixed with _TRUNC_

  For sites using SQL Server or DB2 database management systems, ***Optim*** now supports database relationships with names up to a length of 128 bytes.

- **Litigation Hold**

  You can use ***Optim's*** Litigation Hold to protect information in an Archive File for legal inquiry or investigation. Litigation Hold prevents deletion of the file and supersedes any retention setting. This option is available from the Archive Directory Maintenance dialog for files stored on the Hitachi Content Archive Platform or a Centera backup device.

- **Data Privacy Enhancements**

  Optim Data Privacy features now include the Shuffle function. Shuffle takes a column value and replaces it with a value for the same column from a different row. You can use Shuffle for a single column or multiple columns.

  Modifications have been made to the syntax of the Lookup, Hash Lookup, and Random Lookup functions.

  Data Privacy functions are now licensed separately.

- **Installation Enhancements**

  When configuring ***Optim,*** steps to create a PST directory or DB alias have been reworked to make these processes easier to use.

  You can now use a task on the configuration menu to drop, load or refresh data privacy tables or data.

Expanded Support for *Optim* Server

The ***Optim Server*** can now be deployed on Red Hat Linux 4.0 AS.

Support for DBMS Versions

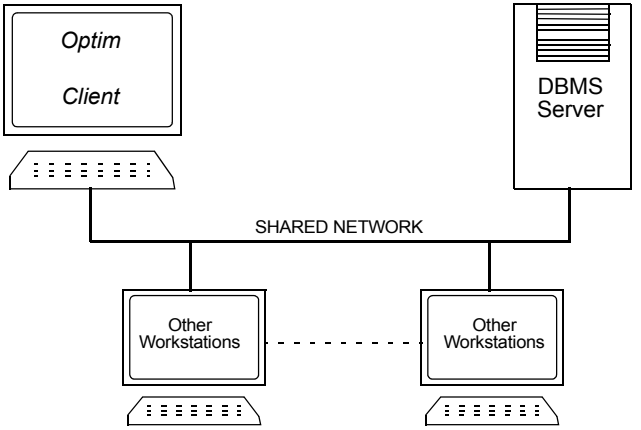
Optim now supports DB2 v9 and Sybase ASE v15.

1. Getting Started

This guide describes the programs used to install and configure the ***Optim*** solution. The **Setup** program guides you through the installation process, and the **Configuration** program prepares your databases and workstations to use ***Optim***.

1.1 Conceptual Overview

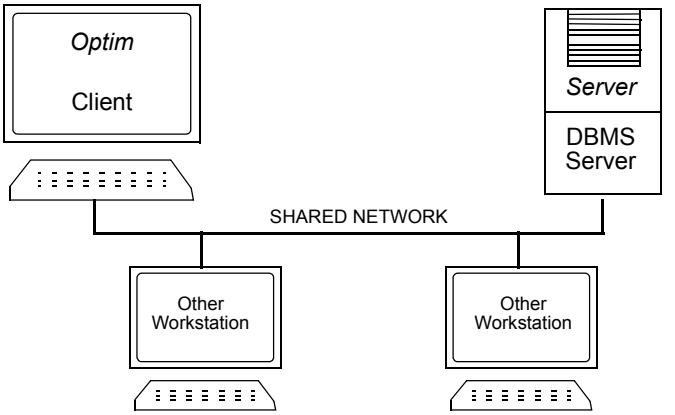
In the simplest configuration, ***Optim*** operates as a client application with all processing taking place directly on the Windows workstation. Unless the database is installed locally, the appropriate DBMS client software is used to communicate with the remote database over a network.



All ***Optim*** data flows over shared network along with other traffic.

However, a different configuration may be desirable when network traffic generated by ***Optim*** competes with other network use, or when workstation capacity (processor, memory, or disk space) causes some tasks to be inefficient or impossible to accomplish. Also, a different configuration is required if processing data from a database in a UNIX® or Linux® environment.

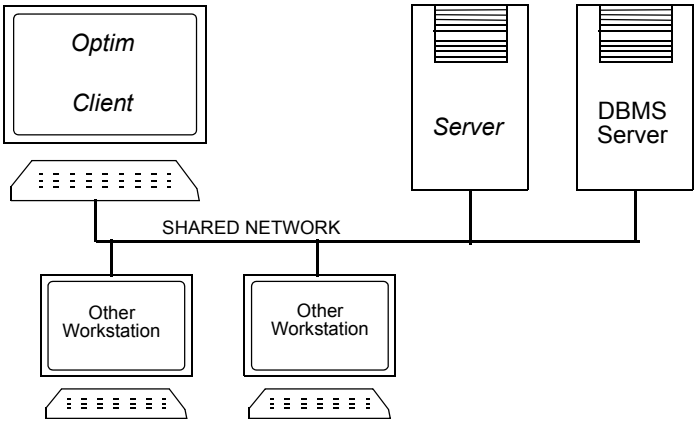
The ***Optim Server*** (***Server***) allows users to define tasks on a Windows workstation, and direct resource-intensive data processing functions to a machine more suited to the task. When a task requires the movement, processing or storage of very large volumes of data, the request can be defined at the workstation in the normal way, then directed for remote processing on the machine hosting the ***Server***.



Minimal ***Optim*** data flows over shared network;
most data stays within the ***Server***/DBMS Server.

The ***Server*** can be installed and run on a Microsoft Windows, Sun Solaris, Hewlett-Packard HP-UX, or IBM AIX platform, or on a Red Hat Application Server. If this machine is the machine on which the database is running, network traffic associated with the movement of

data is eliminated. You can also install the ***Server*** on a machine dedicated to the ***Server*** function.



Minimal ***Optim*** data flows over shared network;
most data flows between the ***Server*** and the DBMS Server.

A dedicated server must have connectivity to the database, but can be configured to avoid competition with other network traffic. In general, a process must be defined using ***Optim*** running on a Windows platform. However, a process can be initiated on any platform, using the Command Line Interface.

Installation and Configuration Sequence

Regardless of the configuration you choose, you must first install ***Optim*** on a Windows machine that has connectivity to your database (i.e., the "First Workstation"). Following this installation, you will **Configure the First Workstation** to create the ***Optim*** Directory and any DB Aliases needed to access your databases. If the First Workstation is to be used as a ***Server***, you can also configure it for this. You can then install and configure any additional Windows-based workstations or ***Servers*** (using the **Configure Additional Workstation** task and, if needed, following the steps for ***Server*** configuration).

If you are implementing the ***Server*** on a UNIX or Linux-based machine, you can follow the directions in **Appendix A. Install and Configure the Server under UNIX or Linux** once the Windows installations are complete and ***Optim*** Directory and DB Aliases are configured.

Several steps are involved in installing ***Optim***. This overview explains these steps, discusses the software and environmental requirements for using the application software, and describes the information you must prepare for the installation and configuration process.

1.1.1 Installation Phase

The installation process unloads ***Optim*** from the installation CD to the target workstation and additional workstations or servers.

You begin the installation phase by using the **Setup** program to load the application software at the first workstation. In **Setup**, you must enter your company name and the identification number indicated in the email sent when ***Optim*** is shipped to you. You must also designate a destination directory for the application software.

In a Windows installation, **Setup** launches a command line application to shut down any ***Optim*** applications that are running. (See **Command Line Application Display** in **Section 2. Installation Setup** for information needed to change the display setting for a command line application.)

Depending on your license agreement, after you install and configure ***Optim***, you may have access to one or more of the following components:

- ***Archive*** allows you to identify and archive sets of relationally intact data before removing selected data from your database. You can browse, search, or restore selected subsets of archived data.
- ***Move*** allows you to identify and extract, migrate, and process sets of relationally intact data. You can create test databases that are referentially complete subsets of a production database, copy sets of related data from a production database to a work area before revising and moving data to the production database, or migrate subsets of data that require data transformations as part of the migration.
- ***Edit*** allows you to edit and browse related data, review logical application paths, resolve data problems, modify data to test all possible scenarios, and ensure that one or more related tables contain expected data.
- ***Compare*** allows you to compare *before* and *after* images of relationally intact sets of data from a set of tables. You can identify and analyze changes to related rows to resolve referential integrity issues or identify similarities and differences between two independent databases and verify database changes.
- ***Scheduler*** allows you to schedule process requests to be executed in unattended mode.

- The ***Configuration*** program allows you to configure the first and additional workstations to use ***Optim***. You can also establish security and perform various tasks to maintain the system environment.
- The ***Server*** allows you to process resource-intensive tasks away from the workstations to reduce network traffic and improve efficiency, to process data that resides in a UNIX or Linux environment, or to use ***Optim*** **Open Data Manager** to access archived data.
- **Open Data Manager** (ODM) provides Archive File access for programs that use the ODBC and JDBC APIs.

Workstations or File Server

You can install ***Optim*** on individual workstations or on a file server for multiple users to share.

Note: Installing ***Optim*** on a file server is different from installing the optional ***Server***. Sites that consider installing ***Optim*** on a file server would generally tend to be unconcerned with the volume of network traffic and, therefore, may not derive any benefit from remote processing on the ***Server***.

Your decision to install ***Optim*** on individual workstations or on a file server does not affect licensing requirements, but there are considerations for either method. The advantages of installing on individual workstations include:

- Improved performance (the executables are not loaded across a network).
- Users are not affected by an upgrade made on the file server.
- Old images are not in use while installing, configuring, or upgrading the software.

In contrast, a single installation on a file server offers the following advantage:

- Ease of administration, both at installation and when applying maintenance or upgrades.

Regardless of your choice, you should install and configure each additional workstation to create desktop shortcuts and create necessary Windows registry entries.

1.1.2 Configuration Phase

The configuration process creates an ***Optim*** Directory, establishes connectivity to the databases accessed by ***Optim***, and supports other maintenance tasks. The ***Optim*** Directory is a set of tables that store all the ***Optim***-specific object definitions you create. Typically, a site uses one shared ***Optim*** Directory, regardless of the number of database instances to be accessed or the number of workstations using ***Optim***. However, you may create as many ***Optim*** Directories as needed to satisfy your site requirements.

The configuration phase consists of configuring the first workstation, configuring each additional workstation and, if licensed, configuring the ***Server*** component.

- **Configure the First Workstation** allows you to confirm the Product License Key and create the components shared by all workstations. For example, only one ***Optim*** Directory and one Product Configuration File are needed, although you may have more than one of each. (Typically, all users share one Product Configuration File, which provides the Product Option settings for your site.)
- **Configure Additional Workstation** allows you to configure each workstation to share components created when the first workstation was configured. You may also specify Personal Option settings for each workstation that are recorded in the Windows registry.
- Configure the ***Server*** on one or more Windows, Solaris, HP-UX, or AIX machines.

Configure First Workstation

Several steps are involved in configuring the first workstation. Each step is briefly described in the following paragraphs.

Note: Before you configure a workstation to use ***Optim***, the DBMS client software must be installed and you must define the information necessary to connect to the database. You must configure the DBMS client software on each workstation to permit access to individual database instances.

Product License Key

The 30-character Product License Key determines the ***Optim*** features your company is allowed to use. This key is unique to your company and is sent to you by E-mail when ***Optim*** is shipped. You must use this

key when you configure the first workstation and any additional workstations.

Note: During the process to configure the first workstation, you can optionally export the Product License Key and other details and import this information when configuring additional workstations.

Create *Optim* Directory

Although you may use any number of database instances with ***Optim***, only one is designated to hold the ***Optim*** Directory. Typically, the Directory will share an instance used for other tables. While the ***Optim*** Directory is rarely so large or so heavily accessed as to justify a dedicated database instance, you can dedicate a database instance solely to the ***Optim*** Directory, if desired.

When you create the ***Optim*** Directory, you are prompted for the following information:

***Optim* Directory**	Any meaningful name (up to 12 characters).
DBMS Type and Version	Supported database management systems include DB2, Oracle, Sybase ASE, SQL Server, and Informix.
Connection Information	User ID and password needed to connect to the database instance and the connection string needed to permit user access.
Table Information	Identifier (**Creator ID**, **Owner ID**, or **Schema Name**) for the ***Optim*** Directory tables and the tablespace where they are created. This identifier is used as a qualifier for the names of plans, packages, or procedures needed to access these tables. The plans, packages, or procedures are created as part of the configuration process.

Note: When you create the ***Optim*** Directory, the **Configuration** program also creates the Windows registry entry needed to access the ***Optim*** Directory.

Create DB Alias(es)

Optim requires a DB Alias for each database instance it accesses. You may define one or more DB Aliases at installation or use the **Configuration** program to add DB Aliases later.

The same information specified for the ***Optim*** Directory is needed for each DB Alias; that is, **DBMS Type** and **Version**, **User ID**, **Password**, **Connection String**, and **Identifier** for the packages, plans, or

procedures to be included as part of the DB Alias definition. Meaningful DB Alias names are desirable because ***Optim*** references tables using a three-part name (*dbalias.ownerid.tablename*).

Create *Optim* Primary Keys

Many ***Optim*** processes require primary keys. Often, database tables do not have DBMS primary keys. In this step, you can create ***Optim*** Primary Keys for any table that does not have one, but does have a unique index. You may choose this option for each DB Alias.

Load Sample Database Tables

Optim is distributed with a sample database, consisting of several tables (CUSTOMERS, ORDERS, etc.). These sample tables allow you to experiment while learning how to use ***Optim*** and serve as the basis for training.

Load Data Privacy Data Tables

Data privacy data tables are available to clients who have an ***Optim*** Data Privacy License. These tables allow you to mask company and personal data — such as employee names, customer names, social security numbers, credit card numbers, and e-mail addresses — to generate transformed data that is both valid and unique.

Initialize and Enable *Optim* Security

Optim Security allows you to secure objects in an ***Optim*** Directory, to control access to data in Archive Files, and to limit the ability of users to create objects or perform functions by assigning access permissions. To use ***Optim*** Security, you must first initialize and enable security for the ***Optim*** Directory and assign a Security Administrator. The Security Administrator can enable or disable security and establish default security settings for the ***Optim*** Directory.

Create Product Configuration File

Most installations create and use one Product Configuration File that establishes Product Options for your site. As part of this step, you can modify the Product Options maintained in the file and edit Personal Options for the workstation.

You can edit Product and Personal Options from within ***Optim***, although it is a good idea to establish the directories to store work and temporary files during the configuration process. These directories are personal in nature and most users specify a directory on their workstation.

Export Registry Data

When you configure the first workstation, you create the ***Optim*** Directory, and the **Configuration** program creates a registry entry that allows ***Optim*** to connect to the ***Optim*** Directory from that workstation. If you are planning to configure one or more additional workstations, you can export the ***Optim*** Directory registry entries and the Product License information to a file. You can save time by importing this file when you configure each additional workstation.

Configure Additional Workstations

After you complete the full installation and configuration for the first workstation, you must configure any other workstations that are to use ***Optim***.

Note: Before configuring a workstation to use ***Optim***, you must configure the DBMS client software on the workstation to permit access to individual database instances.

Run Setup

Even if you decide to install ***Optim*** on a file server, you can run **Setup** before configuring each additional workstation to create application shortcuts. Next, select the **Configure Additional Workstation** option for each workstation.

Import Registry Data

If you exported registry settings to a file when you configured the first workstation, you can import these settings to configure each additional workstation. However, if you do not choose to export and import ***Optim*** Directory registry data, you must follow the flow in the configuration process to create a registry entry.

Configuration Process

When you configure an additional workstation and do not import registry data, you must provide the Product License Key and information needed to create a new Windows registry entry for the additional workstation. The registry entry allows ***Optim*** to connect to the ***Optim*** Directory from the workstation.

Product Configuration File

The last step in configuring each additional workstation is to identify an existing Product Configuration File (created when you configured the first workstation). You may modify Product and Personal Options, if desired.

Configure the *Server*

After you complete the installation and configuration for a Windows workstation that is to use ***Optim***, you can choose to configure the ***Server*** on it. Alternatively, you can install the ***Server*** from a console and use the Command Line Interface to configure the ***Server*** in the appropriate UNIX or Linux environment. (See **Appendix A. Install and Configure the Server under UNIX or Linux** for complete information.)

On a Windows machine, the **Optim Server Settings** dialog, available from the Windows Control Panel, allows you to configure and establish network connectivity between delegating workstations and machines hosting the ***Server***. In addition, the workstations and any machine

hosting the ***Server*** must have connectivity to the database containing the ***Optim*** Directory as well as the database containing data to be processed.

A ***Server*** must have Language Settings for each workstation that accesses it. In a purely Windows environment, you can use Regional Settings from the Windows Control Panel on the machine hosting the ***Server*** to ensure that all needed locales are installed. Installations that include one or more UNIX or Linux-based ***Servers*** translate locales between environments, using a file (locale.conf) that is installed with ***Optim***. Depending upon the environment, the locale.conf file is located in .../IBM Optim/RT/BIN or $(PSTHOME)\etc. You may review the list of locale translations in locale.conf and, if needed, add translations for non-standard locales. See **Section 1.2.4 Character Formats** for more information.

Control Panel

When the installation is complete, select **Optim** from the Windows Control Panel to configure the ***Server***. You can provide settings unique to the server, such as the path and executable file name for each database loader, connection strings for all defined DB Aliases, and protocols for access to the server.

Merge Current User

If desired, you can click **Merge Current User** to copy the Personal Options settings from the registry of the current user to the ***Server*** configuration.

Maintenance Tasks

The Configuration **Tasks** menu offers a number of commands that allow you to maintain the ***Optim*** environment. Some tasks are also used to configure the first and additional workstations.

1.2 Planning for Installation and Configuration

Before you install ***Optim***, you must:

- Decide whether to install on each workstation or on a file server accessed by each workstation.
- Decide upon the installation directory.
- Determine if any database for which you must create a DB Alias supports Unicode data, choose the database instance for the ***Optim*** Directory, and determine a User ID and password for each workstation to access the ***Optim*** Directory.

- Decide whether Functional Security, Object Security, or Archive File Security is to be established for your facility and, if so, broadly identify the network users and groups for which access is allowed or denied.
- Choose an appropriate table identifier (**Creator ID**, **Schema Name**, or **Owner ID**) and database location (tablespace, segment, filegroup, or dbspace) for creating ***Optim*** Directory tables.
- Name a directory folder for the Product Configuration File.
- Ensure that previously installed releases of ***Optim***, particularly the **Scheduler**, are not operating.
- If licensed, decide where to install the ***Server***.

1.2.1 Installation Requirements

Optim is a Windows application. The following software and environment requirements apply.

Software Requirements

Operating System

Client
Microsoft Windows XP Professional
Windows 2000 Professional and Server (Service Pack 4)
Windows 2003 Server

Server
Windows XP Professional
Windows 2000 Professional and Server (Service Pack 4)
Windows 2003 Server
Sun Solaris version 7, 8, 9, or 10
HP-UX version 11i or higher
AIX 5L version 5.1, 5.2, 5.3 (only DB2 and Oracle)
RedHat Linux 3.0 AS, 4.0 AS

DBMS

Optim supports the following database management systems (DBMSs). You must ensure that the version of the DBMS client software is the same as or higher than that for the DBMS server software.

Informix Dynamic Server	7.31, 9.30 (Not supported under AIX.) While ***Optim*** will work with Informix 7.31, the client software must be at least Informix 9.2 or greater. IBM has tested the product with the following versions and found that the product functions properly in an upward-compatible manner as long as no new functionality introduced in the DBMS release is exploited: 9.4 (Toleration Mode Only) 10.1 (Toleration Mode Only)
SQL Server	7.0, 8.0 (2000), 9.0 (2005). (SQL Server does not run on any supported UNIX platforms.) ***Optim*** requires ODBC 3.50 or later to access a SQL Server database.
Oracle	8.1.7 (8i), 9.1 (9i), 9.2 (9i), 10.1 (10g), 10.2 (10g)
Sybase ASE	12.5, 15 Not supported under AIX.
DB2	7.2, 8.1, 8.2, 9.1

You can use ***Optim*** to move data to the DB2 z/OS 7.1 or 8.1 mainframe platform, using an Extract File created either with ***Optim*** or the ***Optim* z/OS Solution**. (The ***Optim* z/OS Solution** cannot process an Extract File created with ***Optim***.)

HP-UX Considerations

On HP-UX PA-RISC architectures, Oracle versions 9i and later provide both 64-bit and 32-bit libraries. The directory for the 32-bit library must be on the 32-bit shared library path (SHLIB_PATH). ***Optim*** supports the HP-UX Itanium architecture in 32-bit emulation mode only.

Solaris Considerations

On Solaris SPARC, Oracle versions 10g and later provide both 64-bit and 32-bit libraries. The directory for the 32-bit library needs to be on the shared library load path (LD_LIBRARY_PATH). ***Optim*** does not support the Solaris x86 architecture.

Solaris and HP-UX Considerations

You must manually edit the ***Optim*** environment setup script rt/rtsetenv, and change the RTORACLELIB environment variable definition in that

file based on your Oracle environment. The shell file rt/rtsetenv contains comments describing how to make the necessary changes.

Hardware Requirements

Optim requires the following hardware:

- Intel® Pentium® or greater (or comparable processor)
- CD-ROM drive (unless installing from a LAN)
- Hard disk space - 400 megabytes
- Disk space for the database - as required
- 256 MB of RAM is recommended. 64 MB minimum is supported. Additional memory enhances performance.

Physical Memory

Physical memory (RAM) requirements depend on the version of Windows you have installed (refer to the system requirements for your Windows version). The actual memory required for acceptable performance will depend on the number of ***Optim*** components that are open (for example, dialogs, ***Optim*** **Server**, ODBC server), as well as the number of open tables, the number of rows being read, and the size of their column data. It will also depend on the memory demands of all other applications and services active on the system. In all cases, it will be greater than the minimum amount of memory suggested by the Windows system requirements.

Virtual Memory

Since Windows is a virtual memory operating system, it can access more memory than actual physical memory. It does this by writing pages (sections of memory) that are not currently referenced to a "page file" on disk. When a page is referenced that is not in memory, Windows loads it back into physical memory. To do this, it must make room for the page by "swapping" it with another page, which in turn is written to the page file. Therefore, the more physical RAM a workstation has, the less swapping needs to be done and performance improves greatly.

The amount of virtual memory (page file space) required will depend on the memory usage of all applications, services, and processes that are running. Having a small amount of physical memory (RAM) means a slower system since time is spent swapping to and from a page file. However, having an insufficient amount of disk space allocated for virtual memory can cause one or more applications or even Windows itself to hang or terminate, sometimes with disastrous results.

For the 2000 and XP versions of Windows, the disk drives and amount of disk space reserved for the paging file (virtual memory) can be limited by user settings that can impact stability. You can view or change this value. Go to System Properties > Advanced tab > Performance Settings button > Advanced tab.

1.2.2 Required Database Permissions

The user account used to perform the ***Optim*** Configuration requires specific database permissions (for example, to allow tables and procedures to be created). This section describes the required permissions for the database management systems that ***Optim*** supports.

Oracle

When you use the Configuration program to create the ***Optim*** Directory tables and procedures, create a DB Alias, and load the sample tables for an Oracle database, the user account must have the following permissions:

CREATE PROCEDURE
CREATE TABLE
CREATE SESSION
UNLIMITED TABLESPACE
SELECT ANY DICTIONARY

Note: The SELECT ANY DICTIONARY permission can be granted to PUBLIC to satisfy the requirement. If the Oracle Initialization parameter 07_DICTIONARY_ACCESSIBILITY is set to TRUE, the SELECT ANY TABLE permission can be used instead of the SELECT ANY DICTIONARY permission.

The above permissions cannot be revoked for the user account once the ***Optim*** Directory or DB Alias is created. Oracle packages are run under the permissions of the user account that created them. If any of the required permissions are revoked, the packages become invalid when executed.

When you create the packages for the ***Optim*** Directory and the Data Dictionary, you can specify a grant authorization ID. When this ID is PUBLIC (the default value), all users are able to run ***Optim***. Optionally, you can specify a user ID or group name to limit access to specific users.

SQL Server

In SQL Server, the user must have a LOGIN at the database server level and a user account for the database instance being accessed. This is true for both creating and accessing an ***Optim*** Directory and a DB Alias.

If shared (global) stored procedures are used for DB Aliases, the user account used to create the stored procedures must have database owner privileges (dbo).

When you catalog the procedures for the ***Optim*** Directory and the system tables, you can specify a grant authorization ID. When this ID is PUBLIC (the default value), all users are able to run ***Optim***. Optionally, you can specify a user ID or group name to limit access to specific users.

Sybase ASE

To create the *Optim* Directory in Sybase ASE, the following must be true:

1. You must connect to the database as the System Administrator (SA), a user account with SA role, a user account with dbo alias.

   Note: The account used to connect to the database may be different from the Owner ID for the ***Optim*** Directory tables.

2. The Owner ID for the ***Optim*** Directory tables must be a valid user account for the database and must have a LOGIN to the database server. If desired, you may specify the special Sybase ID of dbo as the Owner ID of the ***Optim*** Directory tables and related stored procedures.

   Note: The Owner ID may be different from the ID used to connect.

3. If the user account that corresponds to the ***Optim*** Directory table Owner ID does not have SA role, the user account must have the following permissions:

   CREATE TABLE
   CREATE PROCEDURE

To create a DB Alias in Sybase ASE, the following must be true:

1. You must connect to the database as the System Administrator (SA), a user account with SA role, a user account with a dbo alias, or a user account with CREATE PROCEDURE permission.

   Note: The account used to connect to the database may be different from the Owner ID for the procedures used to access the system tables.

2. The Owner ID for the procedures used to access the system tables must be a valid user ID for the database and must have a LOGIN to the database server. If desired, you can specify the special Sybase ID of dbo as the Owner ID of the stored procedures.

   Note: The Owner ID may be different from the ID used to connect.

3. If the Owner ID for the procedures used to access the system tables does not have the SA role, then the user account must have the following permission:

   CREATE PROCEDURE

When you catalog the procedures for the ***Optim*** Directory and the system tables, you can specify a grant authorization ID. When this ID is PUBLIC (the default value), all users are able to run ***Optim***. Optionally, you can specify a user ID or group name to limit access to specific users.

Informix

The Informix utility program, SELNET 32, includes an environment variable named IFX_AUTO_FREE. This variable must not be set. If the IFX_AUTO_FREE variable has a value, the ***Optim*** Configuration program fails during the creation of the ***Optim*** Directory with the error, -481 SQL State 37000 Invalid Statement Name. To avoid or correct the error, ensure that the IFX_AUTO_FREE variable is not set.

Optim uses the ODBC module ISQLT09A.DLL to connect to an Informix server. This module is installed as part of the Informix Client SDK 2.2. This SDK must be installed on the workstation for ***Optim*** to communicate with an Informix database. (You can download the Informix Client SDK for free from the Informix web site.)

To create and access an ***Optim*** Directory and a DB Alias, the user account be defined on the server (that is, the operating system). The

user account must be configured in upper-case for an ANSI database and in lower-case for a non-ANSI database. (The server is not case-sensitive.) To create the ***Optim*** Directory or a DB Alias, a user account must have the RESOURCE privilege.

Note: DBA privilege includes RESOURCE privilege.

In some cases, however, Informix requires that the user account used to create the stored procedures (or tables) match the stored procedure qualifier (or table owner ID). This is true even if the user account has DBA privilege. This rule also applies when creating the sample tables or data privacy tables, since a GRANT is issued as part of the creation process.

When you catalog procedures for the ***Optim*** Directory and the system tables, you can specify a grant authorization ID. When this ID is PUBLIC (the default value), all users are able to run ***Optim***. Optionally, you can specify a user ID or group name to limit access to specific users.

To access an existing ***Optim*** Directory or a DB Alias, a user must have CONNECT privilege.

Note: Both DBA and RESOURCE privileges include CONNECT privilege.

DB2 LUW

The DB2 LUW interface used to validate a user account uses restricted APIs. DB2 LUW for Windows 2000 (or above) provides a Windows Service called DB2 Security Server (db2sec.exe). This program must be started on any machine (client or server) on which a user account must be validated. For client machines, this service is necessary only if any connected instance requires client authentication. During installation of a DB2 LUW product, this service is registered with Windows. It is removed during uninstall.

By default, the DB2 Security Server starts automatically when Windows starts. You can start it manually using the Service dialog from the Windows Control Panel or you can enter the following command at the Command Line Interface:

```
NET START DB2NTSECSERVER
```

You can stop the service manually using the Service dialog or you can enter the following command at the Command Line Interface:

```
NET STOP DB2NTSECSERVER
```

If you want to start the service manually at system startup, use the Service dialog in the Windows Control Panel to change the service startup options.

When you create a DB Alias or apply maintenance to an existing DB Alias, the DB2 LUW client software on the workstation must be at the same or higher level as the target database.

Any version of the DB2 LUW client can connect to a version of the DB2 LUW database that is one version lower or two versions higher.

Note: IBM does not support a DBMS client/server configuration that includes an out-of-service version. For example, DB2 UDB version 7 clients connecting to a DB2 UDB version 8 server are no longer supported because version 7 has been withdrawn from service.

To create an ***Optim*** Directory, the following authorizations are needed:

```
CONNECT
CREATETAB
IMPLICIT_SCHEMA
BINDADD
CREATE_NOT_FENCED_ROUTINE
```

To create a DB Alias, the following authorizations are needed:

```
CONNECT
BINDADD
IMPLICIT_SCHEMA
CREATE_NOT_FENCED_ROUTINE
```

To create and load the sample tables or data privacy tables, the following authorizations are needed:

```
CONNECT
CREATETAB
IMPLICIT_SCHEMA
```

When the plans are bound for the ***Optim*** Directory and the System Catalog, you can specify a grant authorization ID. When this ID is PUBLIC (the default value), all users will be able to run ***Optim***.

Optionally, you can specify a user ID or group name to limit access to specific users.

DB2 z/OS

To create a DB Alias for DB2 z/OS, the following authorizations are needed:

GRANT CONNECT TO *userid*
GRANT BINDADD TO *userid*
GRANT CREATE ON COLLECTION * TO *userid*

To create and load the sample tables or data privacy tables for DB2 z/OS, you will need the following authorizations:

GRANT CONNECT TO *userid*
GRANT USE OF TABLESPACE <*tblspace*> TO <*userid*>
GRANT USE OF BUFFERPOOL <*bpname*> TO <*userid*>

1.2.3 Required Server Authorizations

Windows 2000, Windows XP, Windows 2003 Server

On a Windows machine, the ***Optim Server*** can be run as a process or a service. When it is run as a process, the ***Server*** uses the credentials of the current user ID. When it is run as a service and an explicit user ID is used, the ***Server*** requires the user ID to have the following privileges:

- Act as part of the operating system
- Bypass transverse checking
- Increase quotas
- Log on as a batch job
- Replace a process level token.

You must access the Local Security Policy to grant these privileges to the user. You can access the Local Security Policy as follows.

Note: You must be logged on to the Windows machine with a user ID that has administrator rights.

1. From the Control Panel, access the Local Security Policy applet:

   Administrator Tools > Local Security Policy

2. From the Local Security Policy window, select the menu entry:

Policies > User Rights

3. On the User Rights Policy window, select the following entry in the left pane:

   Security Settings > Local Policies > User Rights Assignments

4. Repeat the following steps for each of the five privileges listed above.
   - Select a privilege from the right pane of the Local Security Settings window.
   - If the user (or group) is not already listed in the Assign To list box, select the Add button to add the user (or group) to the list.
   - Ensure that the Local Policy Setting check box is checked for the user (or group).
5. Select the OK button to apply the changes and close the Local Security Policy Setting window.

UNIX Server

For UNIX, Super-User Server credentials are required to change the effective user ID and group ID. During startup, if the filelogon parameter is set to client or server, the effective user ID that started the daemon must be a Super-User (zero).

1.2.4 Character Formats

Optim uses the Unicode character set in dialogs and to process data.

Optim supports the following DBMS character sets:

Oracle

AL16UTF16
AL32UTF8
AR8ISO8859P6
AR8MSWIN1256
BLT8MSWIN1257
CDN8PC863
CL8ISO8859P5
CL8MSWIN1251
EE8ISO8859P2
EE8MSWIN1250
EL8ISO8859P7
EL8MSWIN1253
IW8ISO8859P8
IW8MSWIN1255
JA16SJIS
NEE8ISO8859P4
N8PC865
TR8MSWIN1254
US7ASCII
US8PC437
UTF8
UTF16
VN8MSWIN1258
WE8DEC
WE8ISO8859P1
WE8ISO8859P9
WE8ISO8859P15
WE8MSWIN1252
WE8PC850
WE8PC860
WE8PC863

Sybase ASE	cp437 cp850 cp1250 cp1251 cp1252 cp1253 cp1254 cp1255 cp1256 cp1257 iso_1 iso_2 iso_4 iso_5 iso_6 iso_7 iso_8 iso_9 roman8 UTF8 UTF16
DB2 z/OS	437 850 860 863 865 1252 UTF8 UTF16

DB2 LUW	437 850 860 863 865 936 949 950 964 970 1252 1363 1370 1383 1386 UTF8 UTF16
SQL Server	1252 UTF8 UTF16
Informix	1252

Directories and Files

The names of all directories and files referenced by, generated, or used with ***Optim*** must consist of ASCII characters. This requirement applies to the installation directories for ***Optim***, as well as the ***Optim*** directories (e.g., Temporary Work Directory, Data Directory, and other directories that are identified in Personal and Product Options or when configuring the ***Server***).

All text files generated by ***Optim*** are in Unicode format and you can edit them with a Unicode-compatible text editor such as Microsoft NotePad. ***Optim*** recognizes Byte Order Mark headers in externally generated files and the following encodings:

- UTF-8
- UTF-16
- UTF-32
- ASCII
- Multi-byte

Also, note that you cannot compare Archive Files created before ***Archive for Servers*** version 6.0 with files created using a current

version of ***Optim***, although you can convert early Archive Files and compare data in the resulting Extract Files. In addition, Report Files created with earlier versions of ***Optim*** are not accessible using version 6.*x*.

Optim Server

Every locale (or its translation) that the ***Server*** is required to handle must reside on the ***Server*** machine. In other words, the ***Server*** must have access to the locale of the delegating workstation. A utility, pr0locl.exe, is provided to tell you the locales that are installed on a machine and the locales with which it is compatible. As an example of the output in a Windows environment, see the following:

```
Current operating system: Microsoft Windows XP
C runtime locales are:
  LC_CTYPE    = English_United States.1252
  LC_COLLATE  = English_United States.1252
  LC_NUMERIC  = English_United States.1252
  LC_MONETARY = English_United States.1252
  LC_TIME     = English_United States.1252
Language Environment Variables:
  LC_ALL =
  LANG   =
Windows Locale is:
  LCID      = 1033 (409)
  Code Page = 1252 (4E4)
RT Server requests can run on or from a UNIX
system that has these locales or their derived locales installed
  C
  en_US.ISO8859-1
```

Optim Directories and DB Aliases

Optim supports storing data in single-byte (ASCII), Unicode, and multi-byte character sets. The default character set is single-byte. When you create an ***Optim*** Directory or DB Alias using a database for which ***Optim*** supports Unicode or multi-byte characters, you are prompted to indicate the character format used for storing data. To use DB Aliases with different character sets, the ***Optim*** Directory must be in Unicode format. If you indicate that the DB Alias for the ***Optim*** Directory database should share connection information with the ***Optim*** Directory, the DB Alias must use the same character set as the Directory.

Unicode Support

The ***Optim*** Directory and DB Aliases can be configured to support universal character encoding (Unicode), if character data in your Unicode-enabled database is kept in Unicode format.

Optim supports the Unicode character set for Oracle, Sybase ASE, Microsoft SQL Server, DB2 LUW, and DB2 z/OS databases.

If ***Optim*** processes data in a Unicode-enabled database, the ***Optim*** Directory must also be in a Unicode-enabled database and the ***Optim*** Directory and DB Aliases for Unicode-enabled databases must be flagged during the configuration process.

Oracle

Unicode-enabled Oracle database servers commonly use UTF-8 but may use UTF-16. The Oracle client will typically use a single-byte character set.

Note: Using char semantics from Oracle Unicode Servers for char type columns (longer than 500) and varchar2 type columns (longer than 1000) is not supported in this release.

To prevent any loss of data, the character set used by the database client must be compatible with that of the database server.

Optim enforces this requirement as follows.

- **Version 8*i* Oracle clients.** For release 8*i*, the character set for the Oracle client is set in the NLS_LANG environment variable, for example:

  SET NLS_LANG=AMERICAN_AMERICA.UTF8

  Restart ***Optim*** and/or the Configuration program after making any changes to the character set.

  1. If the client uses a Unicode character set, the database server must also use a Unicode character set. The ***Optim*** Directory must reside in a Unicode-enabled database and the Directory and DB Alias for the database must be configured for Unicode data.

  2. If the database server does not use a Unicode character set, the client cannot use one either. The DB Alias for the database must not be configured for Unicode data.

  3. If the database server uses a Unicode character set and the client does not, an error results.

- **Version 9.0 and later Oracle clients.** For releases 9.0 and later, the character set for the Oracle client is set in the NLS_LANG environment variable, for example:

  SET NLS_LANG=AMERICAN_AMERICA.AL32UTF8

  Restart ***Optim*** and/or the Configuration program after making any changes to the character set.

- **Version 9.2 and later Oracle clients.**

  1. If the client uses a DB Alias configured for Unicode data to connect to a Unicode database, the client character set is automatically set to match the server character set.

  2. If the client uses a DB Alias that is not configured for Unicode data to connect to a Unicode database, an error results.

  3. If the client uses a DB Alias that is not configured for Unicode data to connect to a non-Unicode database, the client character set is automatically set to match that of the server. (See **Section 1.2.4 Character Formats** for a list of supported character sets.)

  4. If the client uses a DB Alias that is configured for Unicode data to connect to a non-Unicode database, an error results.

  5. If the workstation for the Oracle client uses a non-Unicode character set that is not supported by ***Optim***, an error results.

  6. If the character set for the database server is not supported, an error results.

Microsoft SQL Server

Because SQL Server does not differentiate on the basis of Unicode characteristics, you need not indicate whether an SQL Server ***Optim*** Directory or DB Alias is kept in Unicode format. However, the following rules apply:

1. A ***Optim*** Directory in an SQL Server database is kept in Unicode format. You must indicate whether any DB Aliases for Unicode-supported databases are to be kept in Unicode format.

2. A DB Alias for an SQL Server database must use the same character format as the ***Optim*** Directory.

Sybase ASE

To prevent any loss of data, the character set used by the Sybase ASE database client must be compatible with that of the database server. ***Optim*** enforces this requirement as follows:

1. If the client uses a DB Alias configured for Unicode data to connect to a Unicode database, the client character set is automatically set to match the server character set.
2. If the client uses a DB Alias that is not configured for Unicode data to connect to a Unicode database, an error results.
3. If the client uses a DB Alias that is configured for Unicode data to connect to a non-Unicode database, an error results.

DB2 LUW

To prevent any loss of data, the character set used by the DB2 LUW database client must be compatible with that of the database server. ***Optim*** enforces this requirement as follows:

1. All DB2 LUW DB Aliases in a DB2 LUW ***Optim*** Directory must have the same Unicode format as the Directory.
2. If the client uses a DB Alias configured for Unicode data to connect to a Unicode database, the client character set is automatically set to match the server character set.
3. If the client uses a DB Alias that is not configured for Unicode data to connect to a Unicode database, an error results.
4. If the client uses a DB Alias that is configured for Unicode data to connect to a non-Unicode database, an error results.
5. DB2 LUW DB Aliases in an Oracle, Sybase ASE, or MS SQL Server ***Optim*** Directory can have different Unicode formats; however, ***Optim*** cannot connect to both a Unicode-enabled DB2 LUW database and a non-Unicode-enabled DB2 LUW database during the same session.

DB2 z/OS

To prevent any loss of data, the character set used by the DB2 z/OS database client must be compatible with that of the database server. ***Optim*** enforces this requirement as follows:

1. All DB2 z/OS DB Aliases in a DB2 z/OS ***Optim*** Directory must have the same Unicode format as the Directory.
2. If the client uses a DB Alias configured for Unicode data to connect to a Unicode database, the client character set is automatically set to match the server character set.

3. If the client uses a DB Alias that is not configured for Unicode data to connect to a Unicode database, an error results.
4. If the client uses a DB Alias that is configured for Unicode data to connect to a non-Unicode database, an error results.
5. DB2 z/OS DB Aliases in an Oracle, Sybase ASE, or MS SQL Server ***Optim*** Directory can have different Unicode formats; however, ***Optim*** cannot connect to both a Unicode-enabled DB2 z/OS database and a non-Unicode-enabled DB2 z/OS database during the same session.

If a DB2 z/OS Tablespace includes both Unicode and non-Unicode tables, you must create a separate DB Alias for each table type, a Unicode DB Alias and a non-Unicode DB Alias.

During Load Processing, you can use only one connection, either Unicode or non-Unicode. You must exit ***Optim*** before switching between a Unicode or non-Unicode connection.

If the Load Process includes UTF-8 characters in table or column names, the Control File will be in UTF-8 format. Before transferring a UTF-8 Control File to a z/OS machine, the file must be converted to binary format. To browse a UTF-8 Control File on a z/OS machine, you must apply IBM SPE APAR OA07685 - ISPF Browse Support for Unicode to the machine.

Informix

Unicode support is not available for Informix. If an ***Optim*** Directory is in an Informix database, all DB Aliases must be non-Unicode.

Multi-byte Support

The ***Optim*** Directory and DB Aliases can be configured to support multi-byte character encoding, if character data in your database is kept in a multi-byte character format.

If ***Optim*** processes data in a multi-byte-enabled database, the ***Optim*** Directory must be in a multi-byte or Unicode-enabled database. The ***Optim*** Directory and DB Aliases for multi-byte-enabled databases must be flagged during the configuration process. An ***Optim*** Directory in multi-byte format supports multi-byte DB Aliases only.

Optim uses the Unicode character set in dialogs and to process information. In some multi-byte character sets (such as Oracle JA16SJIS), multiple characters are mapped to the same Unicode character. When these characters are converted from Unicode back to multi-byte (a round trip), the original character may not be returned. ***Optim*** provides a Product Option (on the **Database** tab) and a Personal

Option (on the **Database** tab) that determine how to handle round trip conversion issues when processing data in a multi-byte database.

To prevent any loss of data, the character set used by the database client must be compatible with that of the database server. ***Optim*** enforces this requirement as follows:

1. If the client uses a DB Alias configured for multi-byte data to connect to a multi-byte database, the client character set is automatically set to match the server character set.

2. If the client uses a DB Alias that is not configured for multi-byte data to connect to a multi-byte database, an error results.

3. When connecting to an ***Optim*** Directory, the client may establish a connection, check the database character set, drop the connection, and re-establish it with a new language setting.

Note: Because Oracle stores character LOBS in UCS2, a 16-byte Unicode format, multi-byte character LOBS may not be stored correctly in a multi-byte database. For more information, refer to your Oracle documentation.

1.3 Troubleshooting Your Installation

The ***Optim*** CD includes several utilities that help you troubleshoot your installation and configuration activities. You run these utilities from the Command Line Interface.

1.3.1 Image Locator Diagnostic Tool

The Image Locator Diagnostic Tool, PN0IMAGE.EXE, is a utility that can aid in locating missing DLLs. The syntax of the command follows:

PN0IMAGE [/R] [/O*filespec*] *imagetolocate*

where

/R	Is an optional switch that creates a cross-reference list of image relationships.
/O	Is an optional switch that causes the output to be sent to the location referenced by *filespec*. Normally output is sent to STDOUT.
imagetolocate	Is the name of the image to find. The name must include the proper extension, DLL or EXE.

If the image is not in the current directory, then it must be fully qualified with the proper path information. This utility can be used to determine which DLL could not be loaded when the following ***Optim*** System error occurs:

```
RetCode: PST_FAILED(-00001) General logic error
ExtCode: ENVERR_BADSPGMLOAD(00231) Load of PST SPGM or
ExtDLL failed
OpsCode: The specified module could not be found.
Token1: PN0DSQ20
Token2: PN0DSQ20
```

To resolve the missing DLL in the above example, perform the following steps:

1. Open a MS-DOS window.
2. Change to the drive and directory where the ***Optim*** software was installed (usually, C:\Program Files\IBM Optim\RT\BIN).
3. Run the Image Locator Diagnostic Tool with the name of the offending module. For example, PN0IMAGE PN0SQ20.DLL.

1.3.2 Oracle Connection Diagnostic Tool

The Oracle Connection Diagnostic Tool, ORACONN.EXE, is a utility that determines if ***Optim*** was installed correctly when it fails to connect to an Oracle database. The syntax of the command follows:

ORACONN *userid password TNSservicename*

where

userid	Is the user ID used to connect to the Oracle database. The user ID must be defined in the Oracle database.
password	Is the password used to connect to the Oracle database. The password must be defined for the specified user ID in the Oracle database.
TNSservicename	Is the name of the service associated with the Oracle database.

To test the connection to an Oracle database, perform the following steps:

1. Open a MS-DOS window.
2. Change to the drive and directory where the ***Optim*** software was installed (usually, C:\Program Files\IBM Optim\RT\BIN).
3. Run the Oracle Connection Diagnostic Tool with the name of the TNS Service to which you wish to connect. For example,

   ORACONN internal password beq-local

1.3.3 Microsoft Debugging Utility

The Microsoft Debugging Utility, USERDUMP.EXE, creates a memory dump for a process. Since the output is quite large (as much as 50 meg), use this tool only at the request of Support.

To display a list of running processes and process IDs, enter

USERDUMP -p

To dump processes associated with a single process ID or image binary file name, enter

USERDUMP [-k] <*ProcessSpec*> [<*TargetDumpFile*>]

To dump processes associated with multiple process IDs or image binary file names, enter

USERDUMP -m [-k] <*ProcessSpec*> [<*ProcessSpec*>...]
[-d <*TargetDumpPath*>]

To dump Win32 GUI processes that appear to hang, enter

USERDUMP -g [-k] [-d <*TargetDumpPath*>]

where

-k	Optionally causes processes to be killed after being dumped.
<*ProcessSpec*>	Is a decimal or 0x-prefixed hex process ID, or the base name and extension (no path) of the image file used to create a process.
<*TargetDumpFile*>	Is a legal Win32 file specification. If not specified, dump files are generated in the current directory using a name based on the image file name.
-d <*TargetDumpPath*>	Is the directory in which the dump files are to be created. The default is the current directory.

For example, to dump the main Toolbox process if that is the one that is hanging, perform the following steps:

1. Open a MS-DOS window.
2. Enter **USERDUMP -p** to get a list of processes and process IDs. Look for the process, PR0TOOL.EXE.
3. Enter **USERDUMP *nnnnn***, where *nnnn* is the process id for PR0TOOL.EXE.

The program will take about 10 or 20 seconds to produce the dump file. A dump file will be created in the current directory (unless you specified a target dump file name) with a name similar to PR0TOOL.DMP.

2. Installation Setup

Installing ***Optim*** takes only a few minutes. The **Setup** program guides you through the installation process. When **Setup** completes, use the **Configuration** program to prepare your workstations to use ***Optim***.

Note: You can find information needed to install and configure the ***Optim Server*** (***Server***) feature of ***Optim*** on a machine using the Solaris operating environment, under SPARC; the HP-UX operating environment; the AIX operating environment; or Red Hat Application Server in **Appendix A. Install and Configure the Server under UNIX or Linux**.

Installing from a Network Drive

You can copy the contents of the ***Optim*** CD to a network drive and then run the **Setup** program from the network drive. To copy to a network drive

1. Create a directory on a network drive.
2. Copy the contents of the ***Optim*** CD to the directory. Copy all of the files in the root of the ***Optim*** CD and all of the files in the directories (including subdirectories) to the network drive.
3. See **2.1 Run Setup** to begin installation.

Command Line Application Display

When **Setup** is run in Windows, a command line application will be launched to shut down any ***Optim*** applications that may be running. Depending on the setting of your workstation, the application can start in either a MS-DOS Window or in Full Screen mode. If the setting for your workstation is to start command line applications in Full Screen mode, it may appear that your system has crashed when **Setup** launches the application. To correct this problem, you can set the property of your MS-DOS windows to run in Window mode and not Full Screen mode.

To change or check the setting for your workstation, perform the following steps:

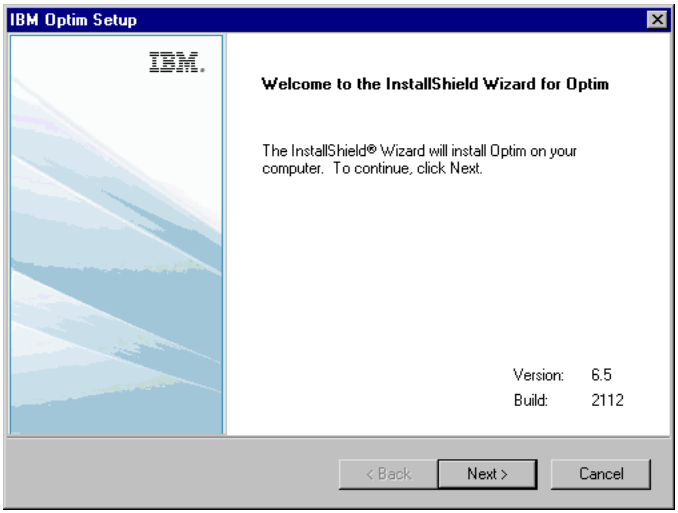
1. From the Start Menu, select Run. In the Run window, enter CMD.EXE and click OK.
2. If a Full Screen MS-DOS session appears, press Alt+Enter to convert the session into an MS-DOS Window. (If an MS-DOS window appears, go to the next step.)
3. Using the mouse, select the C:> icon on the top left corner of the MS-DOS window to display its System Menu.
4. On the System Menu, select Properties. On the Properties window make sure that the Window radio button is selected on the Options tab page. Select OK to save the change.
5. On the Apply Properties window, select the Save properties for future windows with the same title radio button. Select OK to save the change.

2.1 Run Setup

You can begin ***Optim*** installation in one of three ways:

1. Insert the ***Optim*** CD in the workstation drive. ***Optim*** begins the installation automatically.
2. Open Windows Explorer, double-click the icon for your CD drive, and double-click **setup.exe**.
3. Open Network Neighborhood, open the network drive that contains the contents of the ***Optim*** CD you copied, and double-click **setup.exe**.

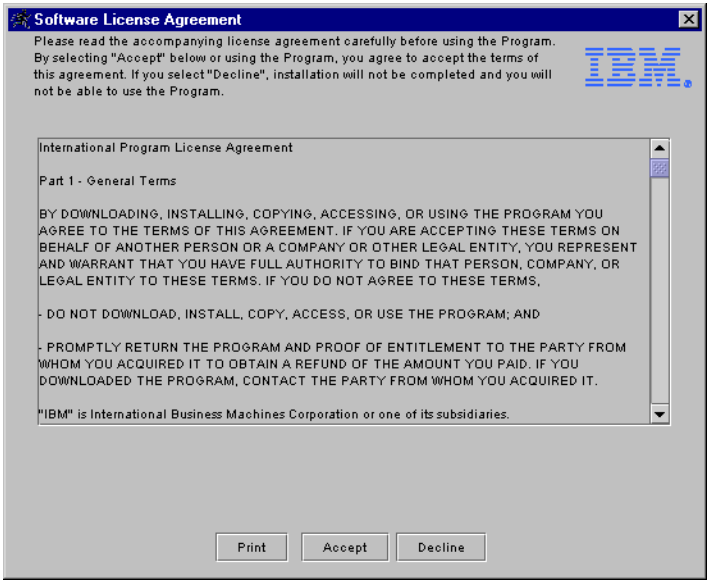
Optim displays the **Welcome** dialog.


IBM Optim Setup
IBM.
Welcome to the InstallShield Wizard for Optim
The InstallShield® Wizard will install Optim on your computer. To continue, click Next.
Version: 6.5
Build: 2112
< Back
Next >
Cancel

After you read the text, click **Next**, to continue.

2.1.1 Software License

The second dialog prompts you to read the License Agreement.


Software License Agreement
Please read the accompanying license agreement carefully before using the Program. By selecting "Accept" below or using the Program, you agree to accept the terms of this agreement. If you select "Decline", installation will not be completed and you will not be able to use the Program.
International Program License Agreement
Part 1 - General Terms
BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, OR USING THE PROGRAM YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON OR A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON, COMPANY, OR LEGAL ENTITY TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,
- DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, OR USE THE PROGRAM; AND
- PROMPTLY RETURN THE PROGRAM AND PROOF OF ENTITLEMENT TO THE PARTY FROM WHOM YOU ACQUIRED IT TO OBTAIN A REFUND OF THE AMOUNT YOU PAID. IF YOU DOWNLOADED THE PROGRAM, CONTACT THE PARTY FROM WHOM YOU ACQUIRED IT.
"IBM" is International Business Machines Corporation or one of its subsidiaries.
Print
Accept
Decline

Command Buttons

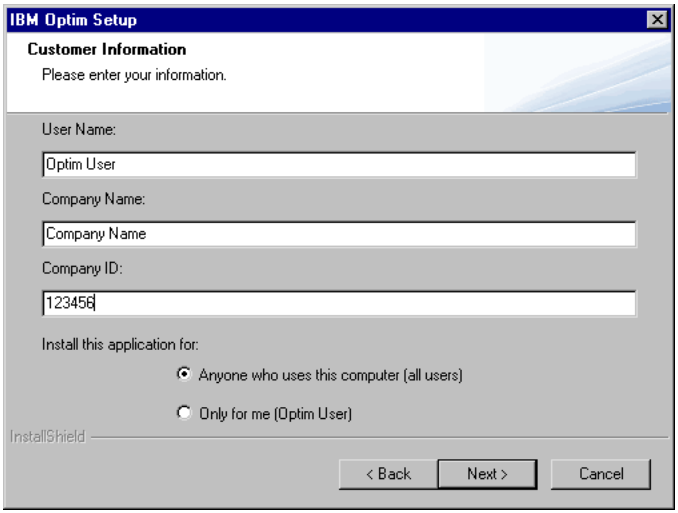
After you read and accept the License Agreement, select **Accept** to indicate that your company agrees to its provisions. You must click **Next** to continue installing ***Optim***. Other command buttons:

Print Prints this dialog.

Decline Cancels **Setup** and does not install ***Optim***.

2.1.2 Customer Information

The **Customer Information** dialog prompts for information to supplement your company License Key.



The following information is needed to proceed with the installation:

User Name Your User ID.

Company Name Your company name, as provided on the notification sent when ***Optim*** is shipped to you.

Company ID Your company identifier, as provided on the notification sent when ***Optim*** is shipped to you.

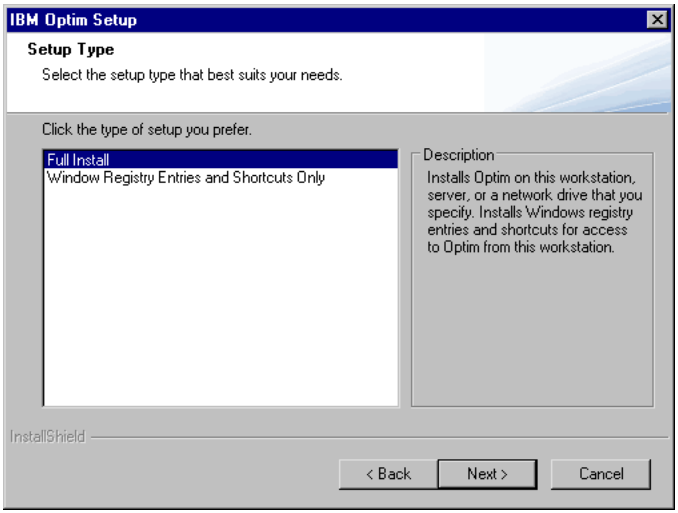
Install this application for

In the lower portion of the dialog, indicate whether you would like the workstation to share the Personal Options and other information in the same registry or use a separate registry for each user. Click **Anyone who uses this computer (all users)** to share the registry information, or click **Only for me** to allow each user to have a private copy of the registry information.

To continue, click **Next**.

2.1.3 Select the Type of Setup

The **Setup Type** dialog prompts you to perform a full install of ***Optim*** or to set up registry entries and shortcuts only.


IBM Optim Setup
Setup Type
Select the setup type that best suits your needs.
Click the type of setup you prefer.
Full Install
Window Registry Entries and Shortcuts Only
Description
Installs Optim on this workstation, server, or a network drive that you specify. Installs Windows registry entries and shortcuts for access to Optim from this workstation.
InstallShield
< Back
Next >
Cancel

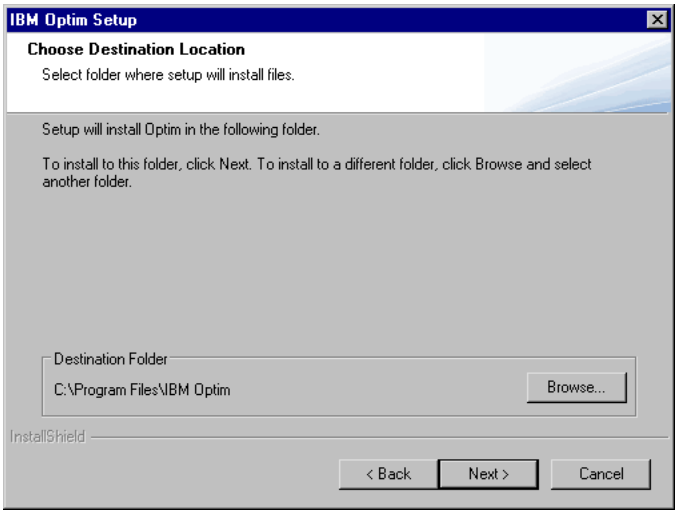
Select **Full Install** to install ***Optim*** on a particular workstation, server, or network drive. This type of setup includes Windows registry entries and shortcuts to access ***Optim*** from the workstation you are using.

Note: If ***Optim*** is already installed on your network, and you want to access it from the workstation you are using, select the option to install **Windows Registry Entries and Shortcuts Only**.

To continue, click **Next**.

2.1.4 Choose Destination Location

The ***Optim*** software must be installed in a destination directory folder. When the **Choose Destination Location** dialog opens, a default Destination Folder is specified. If this folder does not exist, **Setup** creates it as part of the installation process.


IBM Optim Setup
Choose Destination Location
Select folder where setup will install files.
Setup will install Optim in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\Program Files\IBM Optim
Browse...
InstallShield
< Back
Next >
Cancel

Destination Folder Displays the full default directory path for installing ***Optim***. To change this path, click **Browse**. During installation, **Setup** creates subordinate folders, such as **RT\Bin**, within this directory.

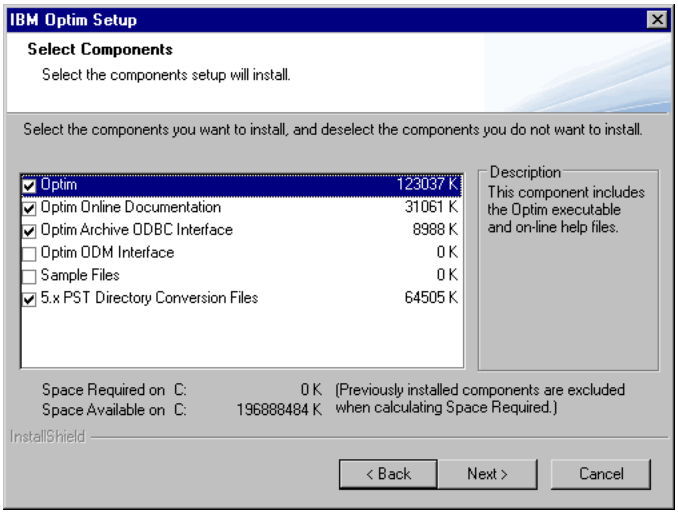
Note: If you are running **Setup** for a workstation with the ***Optim*** software on a file server, you must specify a Directory Folder on the server where the software is installed.

Browse. . . Opens the **Choose Folder** dialog where you can select a different folder for installing ***Optim***.

To continue, click **Next**.

2.1.5 Select Components

The **Select Components** dialog lists the components available for installation.


IBM Optim Setup
Select Components
Select the components setup will install.
Select the components you want to install, and deselect the components you do not want to install.
Optim 123037 K
Optim Online Documentation 31061 K
Optim Archive ODBC Interface 8988 K
Optim ODM Interface 0 K
Sample Files 0 K
5.x PST Directory Conversion Files 64505 K
Description
This component includes the Optim executable and on-line help files.
Space Required on C: 0 K
Space Available on C: 196888484 K
(Previously installed components are excluded when calculating Space Required.)
InstallShield
< Back
Next >
Cancel

Compare the **Space Required** to install the selected components with the **Space Available** in the directory you specified in the **Choose Destination Location** dialog.

Note: If the space available is insufficient for installing the selected components, click **Back** to specify a different destination, or click **Cancel** to quit the installation process.

Optim

Select **Optim** to install the product and the online help files.

Optim Online Documentation

Select **Optim Online Documentation** to install the Introductions, User Manuals, Installation and Configuration Guide, Optim Basic Manual, and Common Elements Manual in PDF format. Additionally, the latest release notice and revision history is included.

Optim Archive ODBC Interface

Select **Optim Archive ODBC Interface** to install version 3.51 of the Open Data Base Connectivity (ODBC) Application Programming Interface (API). Selecting this component registers the ***Optim*** ODBC Interface driver with ODBC on your workstation.

Note: If your workstation has an earlier version of ODBC installed, selecting this component will upgrade the API to ODBC version 3.51.

Optim ODM Interface

Select **Optim ODM Interface** to install Open Data Manager (ODM), which is typically used with integrated applications, such as ***Optim*** **Oracle E-Business Suite Solution**. ODM requires a product license. If you select this option, see **Appendix F. Open Data Manager** for ODM installation instructions.

Sample Files

Select **Sample Files** to install sample Extract, Visual Basic, and Column Map Exit files (see **Appendix H. Samples** for further information).

5.x PST Directory Conversion

5.x PST Directory Conversion is selected by default to install files required for converting PST Directory objects created using version 5.x into a format suitable for use with ***Optim*** version 6.0 and later. See **G.1 Conversion Process for 5.x Optim Directories** on page 567 for details.

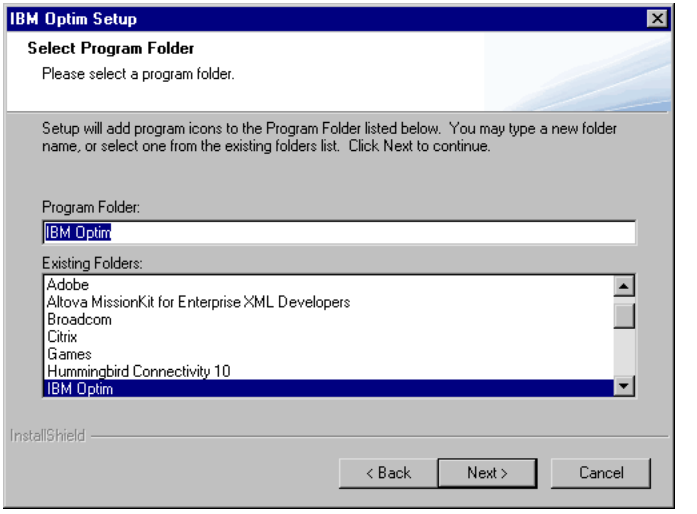
Clear the check box unless you are upgrading from an earlier version of ***Optim***.

To continue, click **Next**.

2.1.6 Select Program Folder

The **Select Program Folder** dialog allows you to specify a folder to hold the program icons for each installed component. The dialog opens with the default name, **IBM Optim**, specified as the Program Folder. You can accept this name, choose a name from the list of **Existing Folders**, or specify a new name.

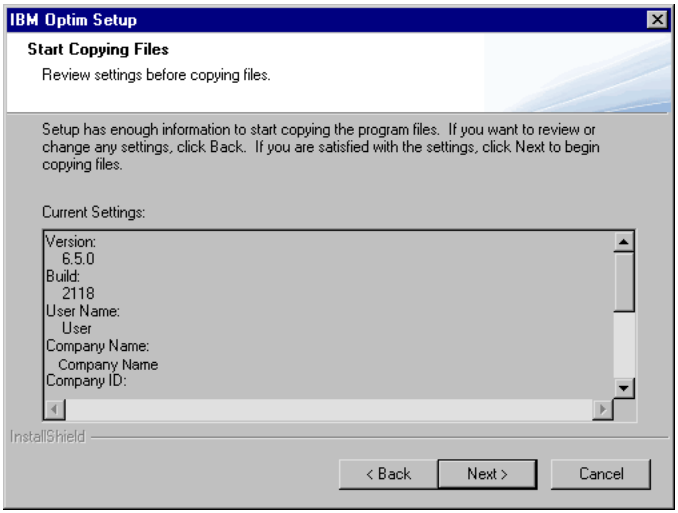
Note: If the specified Program Folder does not exist, **Setup** creates the folder as part of the installation process.


IBM Optim Setup
Select Program Folder
Please select a program folder.
Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing folders list. Click Next to continue.
Program Folder:
IBM Optim
Existing Folders:
Adobe
Altova MissionKit for Enterprise XML Developers
Broadcom
Citrix
Games
Hummingbird Connectivity 10
IBM Optim
InstallShield
< Back
Next >
Cancel

To continue, click **Next**.

2.1.7 Start Copying Files

The **Start Copying Files** dialog displays settings for the current installation. The dialog allows you to review settings before beginning the installation.



To modify settings, click the **Back** button to return to a previously displayed **Setup** program dialog. To begin the installation, click **Next**.

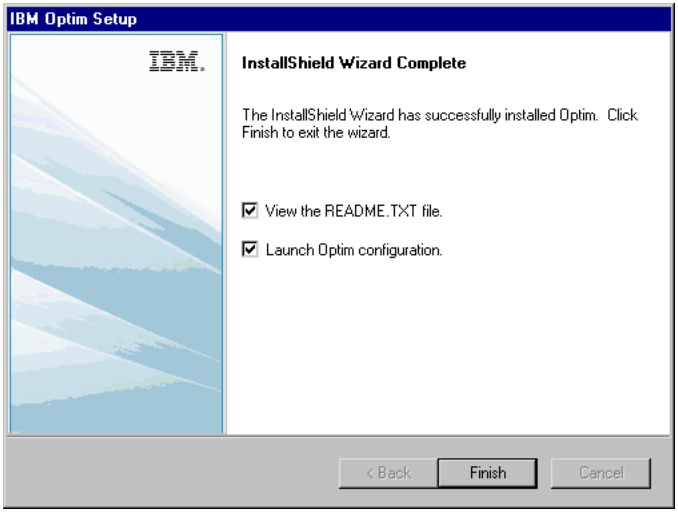
2.1.8 Installation

Setup shuts down any component of ***Optim*** that is running and, during the installation, displays a progress bar to monitor the process. When the files are copied, **Setup** prompts you to install icons on your desktop. Click **Yes** to create the desktop icons, or click **No** to skip this step. Either choice opens the **Setup Complete** dialog.

2.2 Installation Complete

When the installation process is complete, the **Install Complete** dialog allows you to do two things:

- View the README text file for the installed release.
- Launch the ***Optim* Configuration program** and display the **Sign Optim Exit** dialog.
  - The **Sign Optim Exit** dialog allows you to sign the default exit supplied with ***Optim*** or a custom, user-supplied exit of your own creation, as described in **3.5 The Sign Optim Exit Dialog** on page 56. You must sign the default exit or a user-supplied exit to continue with the Configuration process and use ***Optim***.
  - After you sign an exit, the **Configuration** program will launch the ***Optim* Configuration Assistant**, which is described in detail in **4.1.4 Configuration Assistant** on page 71.



Click **Finish** to display the README.TXT file in a separate text editor window and launch the **Configuration** program.

Notes:

- To postpone reading the README.TXT file, clear the **View the README.TXT file** check box before you click **Finish**.

- To postpone the configuration of your installation, clear the **Launch Optim configuration** check box before you click **Finish**.

2.3 Configuration Overview

As noted above, the first step in the Configuration process is to sign a valid exit (i.e., the ***Optim*** default exit or a user-supplied exit). After you do that, the **Configuration** program will create the ***Optim*** Directory, establish connectivity to databases for ***Optim***, and perform other maintenance tasks. The remainder of this manual describes the **Configuration** program and Tasks and explains how to:

- Configure the First Workstation, which includes creating the ***Optim*** Directory and associated DB Aliases, configuring options, and exporting registry data.
- Configure Additional Workstations, which includes importing registry data, creating a registry entry, and specifying a Product Configuration File.
- Configure the ***Optim Server***.
- Use other commands available from the **Tasks** menu.
- Initialize and enable ***Optim*** Security, which includes Archive File Security, Functional Security, and Object Security.

3. Signing an Optim Exit

Optim includes a mechanism that allows you to use a custom exit to apply an additional layer of security to ***Optim***, beyond the extensive security already included in the product, to meet any security requirements mandated by your company or government regulations. This additional security layer is accomplished through a client-supplied exit that identifies who can use ***Optim*** and the executables that each user can run.

Client-supplied exits are called **user-supplied exits** in ***Optim*** to differentiate them from the **default exit** supplied with ***Optim***. The ***Optim*** default exit allows all requests by all users, within the security limitations defined for each user or user group using the security functionality included in ***Optim***.

The default exit is intended for clients who do not need to use a user-supplied exit, although it may also be used temporarily until you create your own, customized exit. If you use the default exit, ***Optim*** user security functions as it did prior to release 6.5.

If you implement a user-supplied exit, that exit will augment the extensive security functionality already included in ***Optim***.

Note: A user-supplied exit may also be used for other functions, such as managing user accounts, monitoring user activity, forcing inactive sessions to timeout, auditing product use, and overriding user authorization credentials.

Regardless of the exit you use (i.e., the default exit or your own exit), you must "sign" that exit before you can use ***Optim***. After the exit is signed, ***Optim*** will invoke the exit at initialization and call it at various "exit points" in the program to determine whether ***Optim*** should continue with what it was about to do. An exit point is a point within a program at which an exit routine can take control to do some external function. The exit allows you to:

- See what is being done by a given user at various points in a program's logic,
- Ensure that the user's request meets your company standards, and
- Change the request, if needed, to pass your company standards or forbid the request altogether.

Optim will call the exit at each exit point to verify that the user's request meets your company standards, such as verifying that the user has permission to run a given executable. The first exit point occurs when the user launches ***Optim***. If you use the exit to provide external security, that exit point determines whether the user has permission to access the product. If the user has the appropriate permissions, the user can continue; if not, ***Optim*** will terminate the user's session after displaying an appropriate error message. (See the **Optim Initialization Exit Programmer's Guide** for a complete list of the ***Optim*** exit points.)

Beginning with ***Optim*** release 6.5, a "signed" exit must exist to use ***Optim***, whether the exit is the ***Optim*** default exit or a user-supplied exit. To sign an exit, you must enter the "company credentials" supplied to your organization when you received ***Optim***. Your company credentials consist of your ***Optim***-supplied company ID, Name, and Password. The ***Optim*** setup process will automatically request these credentials during installation, so you can sign an exit.

Note: If you have write access to the ***Optim*** bin directory and you have the appropriate company credentials, you can change from one exit to another at any time following installation by signing a new exit. You can change from using the default exit to a user-supplied exit (or vice versa), or you can change from one user-supplied exit to another. (If you are switching to user-supplied exit, you must compile, link, and copy that exit to the bin directory before you can sign it.)

The method of signing an exit in a Windows environment differs from the method used in a UNIX environment:

- In a Windows environment, the ***Optim*** **Configuration** program allows you to sign either exit (i.e., the default exit or a user-supplied exit). See **3.3 Signing an Exit in Windows** on page 53 for more information.
- In a UNIX environment, you can only sign the default exit during installation (i.e., during the ***Optim*** **Setup** program). If you want to sign a user-supplied exit, you must run an **opmusign** script file

following installation. (Another script file is available to revert to the default exit from a user-supplied exit, if needed.) See **Appendix A. Install and Configure the Server under UNIX or Linux** for detailed information on signing an exit in UNIX.

The ***Optim*** default exit is delivered unsigned to ensure:

- it is signed by a user with the appropriate company credentials, and
- the person signing the default exit is authorized to make the decision to use that exit, as opposed to a user-supplied exit. This is important because the default exit returns a "continue" code at every exit point. Thus, if the default exit was delivered signed, it would bypass any security checks and additional functionality included your user-supplied exit (assuming you already created one).

3.1 Writing Your Own Exit

If you want to employ the additional functionality available via a user-supplied exit, you must write your own exit. To write an exit, you must do the following:

1. Determine what you want the exit to do.
2. Determine which ***Optim*** *exit points* that call your exit are suitable for what you want to do.
3. Write the appropriate code to respond to those exit points within your user-supplied exit.

After you create an exit, you must compile, link, and copy the exit to the bin directory in which ***Optim*** is installed, before you can sign it. The same is true when you modify an exit. If a signed exit does not exist, you cannot use ***Optim***. (See the **Optim Initialization Exit Programmer's Guide** for more information on creating a user-supplied exit.)

3.2 Prerequisites to Signing a User-Supplied Exit

If you want to use your own, user-supplied exit, the following requirements apply:

- The exit load linked module name must be appropriate for your platform, as shown below:

Platform	Linked Module File Name
Windows	**opmexit.dll**
AIX, Solaris, Linux	**libopmexit.so**
HPUX	**libopmexit.sl**

- You must copy the exit file to the **bin** directory *before* you run the **Configuration** program in Windows.
- The exit file must exist in the **bin** directory and be signed on *every* ***Optim*** installation. Thus, each time you install ***Optim*** in a directory, a signed exit must exist in the bin directory.

Signing Required After Each Install

Unlike the ***Optim*** Security feature, which you must initialize once per ***Optim*** Directory, you must sign an exit *each time you install* ***Optim*** on a machine. Moreover, when you upgrade to a new ***Optim*** release, you must sign a valid exit for each ***Optim*** installation, before you can use ***Optim***. (If you install a new version of ***Optim*** over a previous version, you have to re-copy your exit into the **bin** directory and resign it, or sign the default exit.) The same is true if you reinstall ***Optim***.

Anytime you replace a signed exit executable (i.e., opmexit.dll, libopmexit.so, or libopmexit.sl) with another version of that exit, you must sign the updated exit to use ***Optim***. This is true, even if the executable was previously signed (e.g., in another installation or copied from a backup of a signed exit).

3.3 Signing an Exit in Windows

In Windows, you can use the **Configuration** program to sign either the default exit or a user-supplied exit, although you may also use the **pr0sign** program to sign either exit.

Note: To use ***Optim***, you must sign an exit for each installation of ***Optim*** on a Windows workstation or server. This is also true if you installed multiple copies of ***Optim*** on a single machine. Moreover, if you copy a signed exit from one installation to another, you must sign the exit again at the target installation.

Signing an Exit during Configuration

To sign an exit in Windows, you must run the ***Optim*** **Configuration** program. You also must run the **Configuration** program to switch from using the default exit to a user-supplied exit (or vice versa).

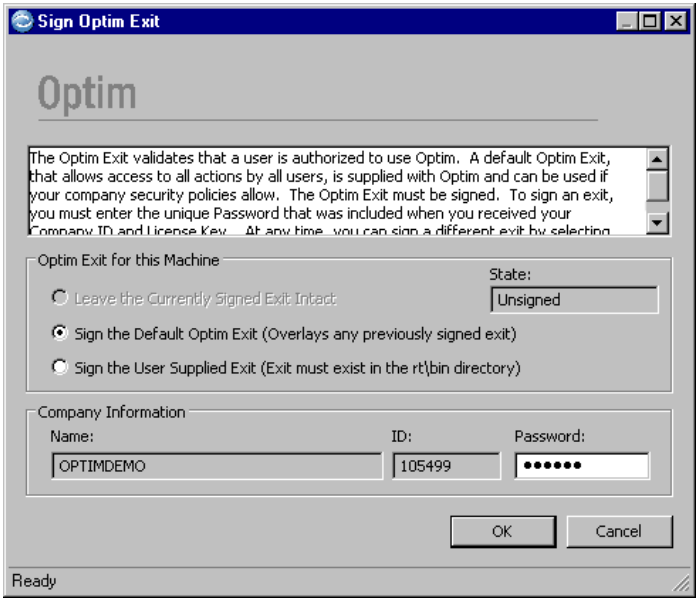
When you install ***Optim***, you can launch the **Configuration** program and display the dialog used to sign an exit by selecting the **Launch Optim configuration** check box on the **Install Complete** dialog, as described in **2.2 Installation Complete** on page 46.

Before you run the **Configuration** program, confirm that no other ***Optim*** processes are running; if other processes are running, shut them down or wait for them finish before you run the **Configuration** program.

If you want to sign a user-supplied exit, you must compile and create the load library **opmexit.dll**. You must then copy the DLL to the **rt/bin** directory ***before*** you run the **Configuration** program.

Note: If you use the **Configuration** program to sign a user-supplied exit, ***Optim*** will immediately call that exit to authorize all future requests. This means that the new exit could theoretically prohibit the current user from executing any other requests, such as running the **Configuration** program, if that user does not have permission to do so in the new exit.

Each time you execute the **Configuration** program, it checks for the existence of a signed exit. If one is not found, the **Sign Optim Exit** dialog displays, and you must sign either the default ***Optim*** exit or a user-supplied exit to use ***Optim***. (See **3.5 The Sign Optim Exit Dialog** on page 56 for further information.)

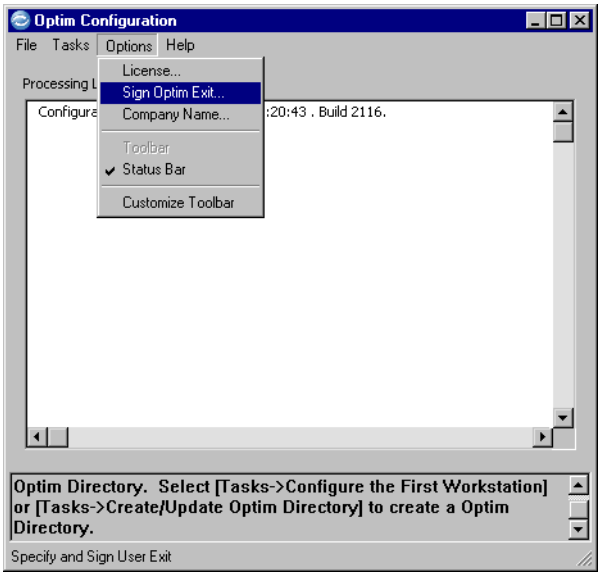

Sign Optim Exit
Optim
The Optim Exit validates that a user is authorized to use Optim. A default Optim Exit, that allows access to all actions by all users, is supplied with Optim and can be used if your company security policies allow. The Optim Exit must be signed. To sign an exit, you must enter the unique Password that was included when you received your
Optim Exit for this Machine
State:
Leave the Currently Signed Exit Intact
Unsigned
Sign the Default Optim Exit (Overlays any previously signed exit)
Sign the User Supplied Exit (Exit must exist in the rt\bin directory)
Company Information
Name:
ID:
Password:
OPTIMDEMO
105499
OK
Cancel
Ready

If you click **Cancel** without signing an exit, ***Optim*** displays a warning message and the **Configuration** program terminates.

Note: If you did not previously provide a company Name and ID, the **Specify Company Name** dialog will appear before the **Sign Optim Exit** dialog. See **3.6 Specifying a Company Name and ID** on page 60 for more information.

3.4 Changing a Signed Optim Exit

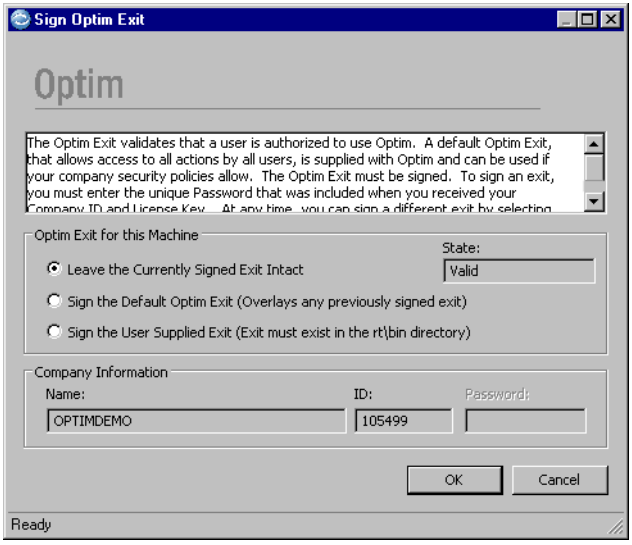
After you sign an exit, you can sign a different exit or switch between the default exit and a user-supplied exit by selecting *Options* > *Sign Optim Exit* from the **Configuration** main window.



Selecting this option displays the **Sign Optim Exit** dialog, described in **3.5 The Sign Optim Exit Dialog** on page 56.

3.5 The Sign Optim Exit Dialog

Optim will automatically display the **Sign Optim Exit** dialog anytime you execute the **Configuration** program if a signed exit does not exist. (You also can manually display that dialog by selecting *Options* > *Sign Optim Exit* from the **Configuration** main window.)


Sign Optim Exit
Optim
The Optim Exit validates that a user is authorized to use Optim. A default Optim Exit, that allows access to all actions by all users, is supplied with Optim and can be used if your company security policies allow. The Optim Exit must be signed. To sign an exit, you must enter the unique Password that was included when you received your
Optim Exit for this Machine
State:
Leave the Currently Signed Exit Intact
Valid
Sign the Default Optim Exit (Overlays any previously signed exit)
Sign the User Supplied Exit (Exit must exist in the rt\bin directory)
Company Information
Name:
ID:
Password:
OPTIMDEMO
105499
OK
Cancel
Ready

The **Sign Optim Exit** dialog includes the following options.

Optim Exit for this Machine

There are three options under the heading **Optim Exit for this Machine**. Click on the option you want to use.

- **Leave the Currently Signed Exit Intact**

  Use this option to leave the currently signed exit in place. You must have permission to execute the **Configuration** program to use this option. This option is available only if an exit was previously signed, in which case the word **Valid** will appear to the right of this option, under **State**.

  If you select this option, the **Password** field is disabled and clicking **OK** or **Cancel** has the same effect (i.e., the existing exit remains in effect.)

  This is the default option when the **State** entry is **Valid**.

- **Sign the Default Optim Exit**

  Use this option to sign the *default* **Optim Exit**. The default exit allows all requests by all users, within the security limitations defined for each user or user group via the security functionality included in ***Optim***. If you select this option, you must specify your company **Password** to sign the default exit.

  Signing the default exit will overlay any previously signed exit. If you are replacing a user-supplied exit, you must have permission in that exit to sign the new exit.

  This is the default option when the **State** entry is **Unsigned**.

- **Sign the User Supplied Exit**

  Use this option to sign a user-supplied exit. (See the **Optim Initialization Exit Programmer's Guide** for information on how to write an exit.) If you select this option, you must specify your company **Password** to sign the user-supplied exit.

  Before you sign a user-supplied exit, you must copy it to the **rt/bin** directory where you installed ***Optim***. This step will overlay any previously signed exit, rendering ***Optim*** unusable until you sign the new exit.

State

This display-only entry identifies the current state of your exit.

Code	Meaning
Unsigned	A signed exit does not exist or was not found. This is the standard status after the initial installation of an ***Optim*** release. You must sign a valid exit to use ***Optim***.
Valid	A signed exit exists. No action is required in response to this status, unless you want to use a different exit.

Corrupt	The existing, signed exit was not the one expected by ***Optim***. The two most common reasons for this status are: • an install was done on top of an existing install that already contained a signed exit • the existing exit was tampered with. If you receive this status, you must re-sign a valid exit to use ***Optim***.
Not Authorized	The current user does not have permission to access the **Configuration** program, so ***Optim*** will terminate the user's session after displaying an appropriate error message. If the user requires access to the **Configuration** program, contact your ***Optim*** Administrator to have the user's access permissions changed.

Company Information

There are three items listed under this heading: company **Name**, **ID**, and **Password**. Each company is assigned a unique company Name, ID, and Password when it receives ***Optim***. These entries are your company credentials for accessing ***Optim***.

When you install ***Optim*** on a Windows machine, you normally enter your company **Name** and **ID** during setup, although this may not be the case in some instances. See **3.6 Specifying a Company Name and ID** on page 60 for more information.

Name

Optim will automatically display the company name assigned to your organization here. (Your ***Optim***-supplied name may not match the spelling or punctuation used in your company's actual name.) You cannot change this entry.

ID

Optim will automatically display the company ID assigned to your organization here. You cannot change this entry.

Password

You must specify the **Password** assigned to your company to sign any exit, whether it be the ***Optim*** default exit or a user-supplied exit. This entry is case sensitive, and you must enter it in the format provided to you when you received ***Optim***.

This entry is required, unless you selected the **Leave the Currently Signed Exit Intact** option.

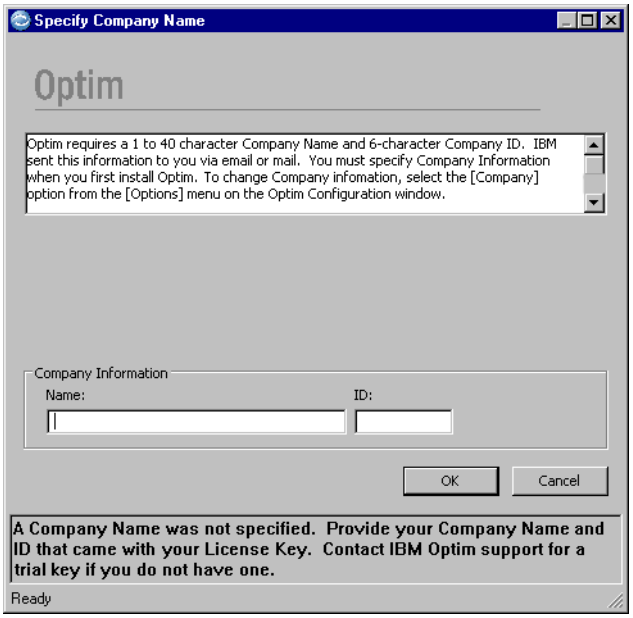
Click OK to sign the selected Exit

After you specify your company password to sign an exit, click **OK** to complete the signing process and close the **Sign Optim Exit** dialog.

Note: You must sign a valid exit to use ***Optim***. If you click **Cancel**, instead of **OK**, and a signed exit does not already exist, ***Optim*** will display a warning message and the **Configuration** program will terminate.

3.6 Specifying a Company Name and ID

The first time you execute the **Configuration** program on a workstation or server, the **Specify Company Name** dialog will appear if you did not previously specify your company **Name** and **ID**. In that case, this dialog will appear before the **Sign Optim Exit** dialog, because a company Name and ID are required to sign an exit.


Specify Company Name
Optim
Optim requires a 1 to 40 character Company Name and 6-character Company ID. IBM sent this information to you via email or mail. You must specify Company Information when you first install Optim. To change Company infomation, select the [Company] option from the [Options] menu on the Optim Configuration window.
Company Information
Name:
ID:
OK
Cancel
A Company Name was not specified. Provide your Company Name and ID that came with your License Key. Contact IBM Optim support for a trial key if you do not have one.
Ready

If this dialog displays, you must specify your company **Name** and **ID** and click **OK** to proceed with the signing process. Both entries are case sensitive, and you must enter both entries in the format provided to you when you received ***Optim***.

4. Configuration Window and Menus

This chapter describes the main window for the ***Optim*** **Configuration** program and certain general configuration functions. The principal configuration tasks are described in the following chapters.

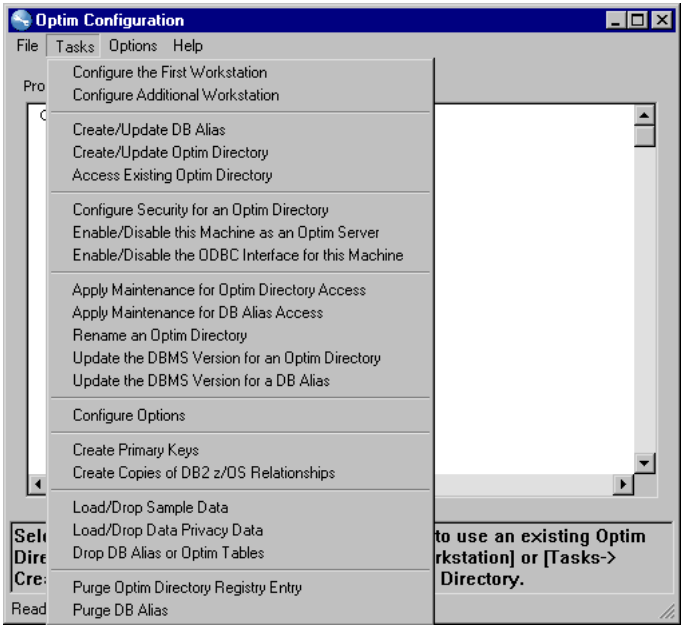
Note: Before you do any configuration functions, you must sign the ***Optim*** default exit or a user-supplied exit of your own creation. You cannot continue with the Configuration process or use ***Optim*** until you sign a valid exit using the **Sign Optim Exit** dialog, as described in **Chapter 3. Signing an Optim Exit**

DBMS Terms

Optim supports several database management systems. Terms used in a configuration dialog reflect the DBMS for the database that is being configured. For example, for an Oracle database, a configuration dialog may refer to *Packages* used to access database tables. However, for a Sybase ASE or SQL Server database, the same dialog refers to *Procedures*, and for a DB2 database it refers to *Plans*. Varying terms are noted in the discussion of a dialog.

4.1 Main Window and Menus

The Configuration main window includes the menu bar, toolbar, Processing Log, message bar, and status bar.


Optim Configuration
File
Tasks
Options
Help
Configure the First Workstation
Configure Additional Workstation
Create/Update DB Alias
Create/Update Optim Directory
Access Existing Optim Directory
Configure Security for an Optim Directory
Enable/Disable this Machine as an Optim Server
Enable/Disable the ODBC Interface for this Machine
Apply Maintenance for Optim Directory Access
Apply Maintenance for DB Alias Access
Rename an Optim Directory
Update the DBMS Version for an Optim Directory
Update the DBMS Version for a DB Alias
Configure Options
Create Primary Keys
Create Copies of DB2 z/OS Relationships
Load/Drop Sample Data
Load/Drop Data Privacy Data
Drop DB Alias or Optim Tables
Purge Optim Directory Registry Entry
Purge DB Alias
to use an existing Optim
rkstation] or [Tasks->
Directory.

Note: When the **Configuration Assistant** or other dialogs are open, the main window is inactive and cannot be used except to view the most recent entries in the Processing Log.

4.1.1 Main Window

The Configuration main window includes the following:

Menu bar	The menus for the **Configuration** program.
Toolbar	Buttons to select Online Help Contents or What's This Help.
Processing Log	A list of actions performed by the **Configuration** program.
Message bar	Basic information to help you select a task or know the outcome of a selected task.

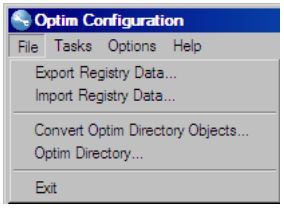
Status bar Messages about a specific command or the current action. The status bar appears at the bottom of the main window and each dialog.

4.1.2 Menus

To use the **Configuration** program, select a command from any menu on the main window menu bar.

File Menu

The **File** menu in the main window lists commands to view or edit information regarding the ***Optim*** Directory, convert ***Optim*** Directory objects when upgrading, or exit the **Configuration** program. In addition, you can select commands to export or import registry data for a particular ***Optim*** Directory.



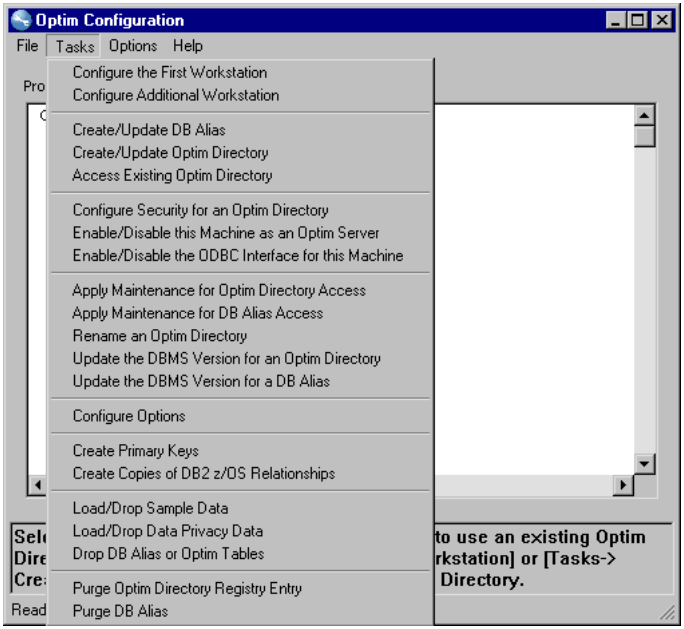
Select any of the following commands:

Export Registry Data You can save time by exporting ***Optim*** Directory registry data to a file and saving the file to a directory that is easily accessible for configuring other workstations. While configuring the first workstation, you are prompted to export registry data, or you can select **Export Registry Data** from the **File** menu on the Configuration main window. See **5.1.6 Export Registry Data** on page 137 for more information.

Import Registry Data	To configure a workstation, you can import ***Optim*** Directory registry data and the Product License Key from a file of information exported from another workstation. You are prompted to import ***Optim*** Directory registry data when configuring each workstation after the first, or you can select **Import Registry Data** from the **File** menu on the Configuration main window. See **5.2.1 Import Registry Entries** on page 141 for more information.
Convert Optim Directory Objects	All ***Optim*** Directories created prior to version 6.0 of ***Archive*** and the ***Relational Tools***, require a conversion to be compatible with later versions. Additionally, any ***Optim*** Directory created prior to ***Optim*** version 6.2 on an SQL Server database must be converted. See **Appendix G. Converting PST and Optim Directory Objects** for more information.
Optim Directory	Connect to or disconnect from an ***Optim*** Directory, or modify a connection.
Exit	Close the Configuration main window.

Tasks Menu

Select commands from the **Tasks** menu to configure and maintain the ***Optim*** environment. You can choose to perform these tasks at any time.


Optim Configuration
File
Tasks
Options
Help
Configure the First Workstation
Configure Additional Workstation
Create/Update DB Alias
Create/Update Optim Directory
Access Existing Optim Directory
Configure Security for an Optim Directory
Enable/Disable this Machine as an Optim Server
Enable/Disable the ODBC Interface for this Machine
Apply Maintenance for Optim Directory Access
Apply Maintenance for DB Alias Access
Rename an Optim Directory
Update the DBMS Version for an Optim Directory
Update the DBMS Version for a DB Alias
Configure Options
Create Primary Keys
Create Copies of DB2 z/OS Relationships
Load/Drop Sample Data
Load/Drop Data Privacy Data
Drop DB Alias or Optim Tables
Purge Optim Directory Registry Entry
Purge DB Alias
to use an existing Optim
rkstation] or [Tasks->
Directory.

Select any of the following commands:

Configure the First Workstation

Confirm the Product License Key after installation and create the components shared by all workstations. Typically, all users on all workstations share one Product Configuration File that contains the Product Options for your site, although you may have more than one of each.

Configure Additional Workstation

Configure each additional workstation on which ***Optim*** is installed to share components created when the first workstation was configured. You may also configure Personal Options for the workstation.

Create/Update DB Alias	A DB Alias is required for each database to which ***Optim*** connects. Use this command to create any DB Aliases that were not created when configuring the first workstation or to update existing DB Aliases.
Create/Update Optim Directory	In most cases, your site will use a single ***Optim*** Directory that is created when the first workstation is configured. Use this task as a step in re-locating the ***Optim*** Directory or when an upgrade to ***Optim*** requires a new Directory.
Access Existing Optim Directory	A workstation must have a Windows Registry entry for the ***Optim*** Directory. This registry entry is created when the workstation is configured, however, additional entries are required for any additional Directories that may be accessed by the workstation. Use this task, which replicates the steps described in **5.2.2 Create Registry Entry** on page 143 to create additional registry entries.
Configure Security for an Optim Directory	You can initialize ***Optim*** Security using the **Configure the First Workstation**, **Create/Update Optim Directory**, and **Configure Options** tasks; however, you must use **Configure Security for a Optim Directory** task to both initialize ***Optim*** Security and enable the security features or to update your security settings.
Enable/Disable this Machine as an Optim Server	Use this task to change the ***Optim Server*** status of a machine.
Enable/Disable the ODBC Interface for this Machine	Use this task to enable or disable the ODBC interface access to Archive Files for a previously configured workstation.

Apply Maintenance for Optim Directory Access	Generally, you must apply maintenance for ***Optim*** Directory access to refresh or update the packages, plans, or procedures needed to access the ***Optim*** Directory tables, when you upgrade ***Optim*** or if you drop the ***Optim*** Directory for some reason.
Apply Maintenance for DB Alias Access	You must apply maintenance for DB Alias access when upgrading ***Optim*** or to refresh packages, plans, or procedures for database access.
Rename an Optim Directory	To rename an ***Optim*** Directory, you must replace the name in the Directory itself and in the Windows registry on each workstation that accesses the Directory. Use this task to change the name in the ***Optim*** Directory and workstation registry or, once the ***Optim*** Directory is changed, to re-name a registry entry or register the re-named Directory on a workstation.
Update DBMS Version for an Optim Directory	Use this task when the database for the ***Optim*** Directory has been upgraded to a new version.
Update DBMS Version for a DB Alias	Use this task when a database has been upgraded.
Configure Options	Typically, the Product Configuration File and the Personal Options registry entries are created when you configure the workstations. Use this task to modify these options.
Create Primary Keys	***Optim*** Primary Keys are usually created when you configure a workstation or create a DB Alias. After you install ***Optim***, you can use this task to create primary keys for tables added to the database.

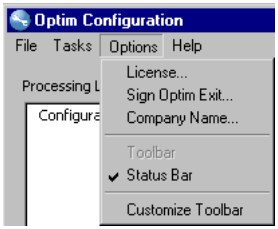
Create Copies of DB2 z/OS Relationships	Use this task to copy DB2 z/OS relationships into the ***Optim*** Directory, which reduces the run time when accessing DB2 z/OS tables.
Load/Drop Sample Data	Sample tables are distributed with ***Optim*** and are generally loaded when you configure a workstation, but you can use this task to load or refresh the sample data independently.
Load/Drop Data Privacy Data	Data privacy data tables are available to clients who have an ***Optim*** Data Privacy License. These tables are generally loaded when you configure a workstation (if you have a Data Privacy License), but you can use this task to load or refresh them.
Drop DB Alias or Optim Tables	Use this task to drop a DB Alias or a ***Optim*** Directory.
Purge Optim Directory Registry Entry	You may, at times, want to remove workstation access to a ***Optim*** Directory, without dropping the Directory or packages, plans, or procedures used to access that Directory or disable ***Optim*** for a workstation. Use this task to purge a workstation registry entry to accomplish these goals.
Purge DB Alias	You may want to purge a DB Alias when you drop a database or to make a database temporarily inaccessible to workstations using ***Optim***.

Note: Many basic tasks are also available when you select **Configuration Assistant** from the **Help** menu. See **4.1.4 Configuration Assistant** for details.

Options Menu

Use the **Options** menu to edit or view license or company name information, sign a user exit, customize the toolbar, and view or hide the

toolbar or status bar by selecting either command from the menu. Select any of the following commands:



License — After the initial installation, you may need to change the license key. A new license key may be required, for example, to activate additional functions or increase the number of users or servers for ***Optim***. Select **License** to display the **Specify Product License Key** dialog.

After you update the license key, you must store the key in the ***Optim*** Directory by connecting to the Directory.

Sign Optim Exit — Select this option to display the **Sign Optim Exit** dialog to sign and activate a new exit, whether it is the ***Optim*** default exit or a user-supplied exit.

Company Name — IBM generates a license key for a specific Company Name and Company ID. Select **Company Name** to display the **Change Company Name** dialog.

Toolbar — Display or hide the toolbar (a check mark indicates it is selected for display).

Status Bar — Display or hide the status bar (a check mark indicates it is selected for display).

Customize Toolbar — Open the **Customize Toolbar** dialog to add or remove buttons.

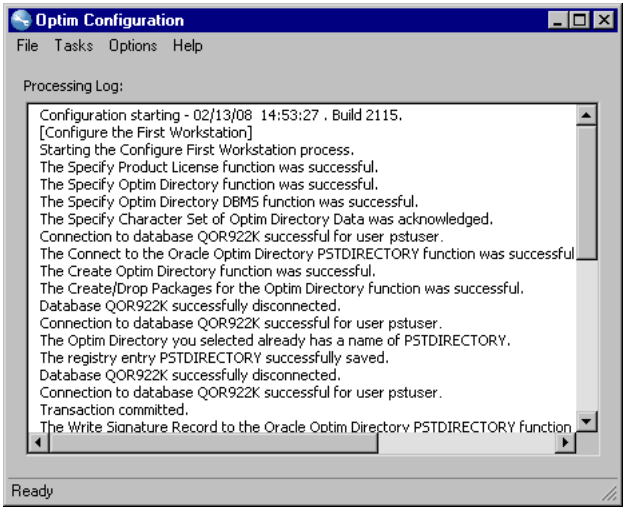
Help Menu

Use the **Help** menu to access online help information or to select the **Configuration Assistant**. In addition, if you have internet access, you can connect directly to the IBM Web site.

(A check mark indicates the toolbar or status bar is selected for display.)

4.1.3 Processing Log

The Processing Log lists the actions performed during the configuration process or when you select any command on the **Tasks** menu.


Optim Configuration
File Tasks Options Help
Processing Log:
Configuration starting - 02/13/08 14:53:27 . Build 2115.
[Configure the First Workstation]
Starting the Configure First Workstation process.
The Specify Product License function was successful.
The Specify Optim Directory function was successful.
The Specify Optim Directory DBMS function was successful.
The Specify Character Set of Optim Directory Data was acknowledged.
Connection to database QOR922K successful for user pstuser.
The Connect to the Oracle Optim Directory PSTDIRECTORY function was successful
The Create Optim Directory function was successful.
The Create/Drop Packages for the Optim Directory function was successful.
Database QOR922K successfully disconnected.
Connection to database QOR922K successful for user pstuser.
The Optim Directory you selected already has a name of PSTDIRECTORY.
The registry entry PSTDIRECTORY successfully saved.
Database QOR922K successfully disconnected.
Connection to database QOR922K successful for user pstuser.
Transaction committed.
The Write Signature Record to the Oracle Optim Directory PSTDIRECTORY function
Ready

Use this log to review the actions in the configuration process and determine if additional action is required. The Processing Log shows the following.

- The date and time you started the **Configuration** program.
- A list of the processes started, completed, or cancelled.
- The tasks performed successfully or unsuccessfully.
- Instances of connecting to or disconnecting from the database.
- The names of newly created ***Optim*** Directory tables.
- The names of newly created database plans, packages, or procedures.
- The sample tables, ***Optim*** objects, and data privacy data tables loaded or dropped.

Note: To keep processing steps in view, you can move the Processing Log window without regard to other open windows.

The **Configuration** program generates a file (**PR0CNFG.LOG**) of configuration information from the current and previous sessions. This file is saved to the **Temporary Work Directory** specified when you configure Personal Options (or in the default Temp directory). If needed, you can browse or print this file using a text editor such as *Notepad*.

4.1.4 Configuration Assistant

There are several ways to start a task to configure ***Optim***.

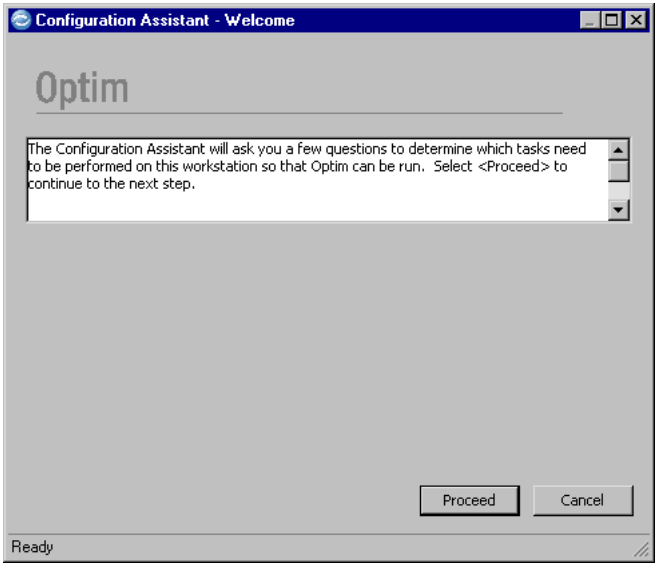
- You can use the **Configuration Assistant**, available immediately following installation when you select the option to **Launch Optim configuration**. The **Configuration Assistant** provides Wizard-like help to guide you to the appropriate configuration options. You may also start the **Configuration Assistant** from the **Help** menu in the **Configuration** program.
- You can select individual configuration options from the **Tasks** menu in the **Configuration** program.

After you install ***Optim***, you are prompted to configure the first workstation. Choosing to continue starts the **Configuration Assistant**. If you choose not to configure immediately after installing the software, you can select **Configure First Workstation** from the **Tasks** menu or select **Configuration Assistant** from the **Help** menu.

Configuration Assistant

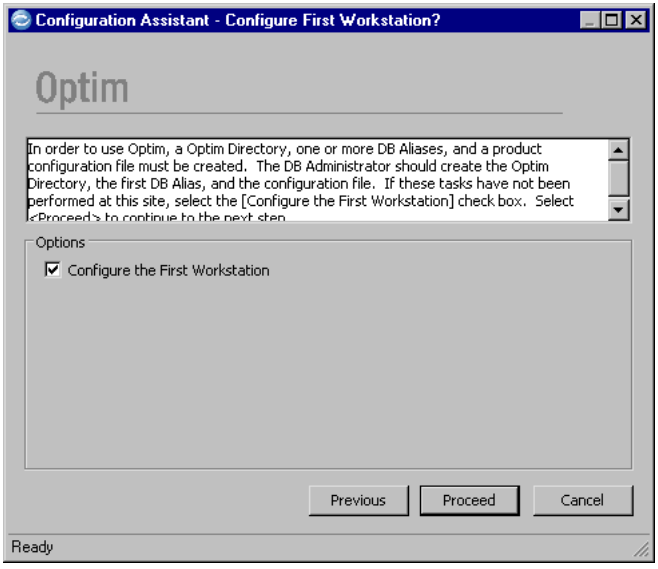
The **Configuration Assistant** presents a series of dialogs to guide you through each step in the configuration process. During the process, you

make selections appropriate to your particular site and circumstances. The first window is the **Welcome** dialog.


Configuration Assistant - Welcome
Optim
The Configuration Assistant will ask you a few questions to determine which tasks need to be performed on this workstation so that Optim can be run. Select <Proceed> to continue to the next step.
Proceed
Cancel
Ready

To continue, click **Proceed**.

The next dialog prompts you to **Configure the First Workstation.**


Configuration Assistant - Configure First Workstation?
Optim
In order to use Optim, a Optim Directory, one or more DB Aliases, and a product configuration file must be created. The DB Administrator should create the Optim Directory, the first DB Alias, and the configuration file. If these tasks have not been performed at this site, select the [Configure the First Workstation] check box. Select
Options
Configure the First Workstation
Previous
Proceed
Cancel
Ready

This dialog and the other dialogs in **Configuration Assistant** are similar to the **Welcome** dialog with the addition of a task check box:

- To perform a task, select the check box and click **Proceed** to open the first dialog for the task.
- To skip a task, clear the check box and click **Proceed** to open the next **Configuration Assistant** dialog.

4.1.5 Dialogs

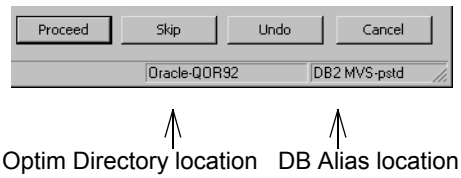
The **Configuration** program presents a series of dialogs to complete a specific task. You respond to prompts or provide necessary information and proceed to the next step in the process.

Some configuration dialogs are used in a number of different tasks; however, only the options appropriate for a specific task are available. In this guide, unavailable options are explained only if certain conditions cause them to become active.

Most configuration dialogs include the following:

- An information (read me) box provides details and directions to guide you through a step in the configuration process.
- Dialog-specific elements prompt for information needed to perform a selected configuration task. When a dialog opens, these elements are populated with default entries or other useful information whenever possible, and the most likely options are pre-selected.
- Command buttons control the logical flow from one dialog to the next.
- The status bar at the bottom of most configuration dialogs displays one or two boxes when you are connected to a database. The first box indicates the location of the ***Optim*** Directory. The second box is displayed if you are also connected to a DB Alias and indicates the corresponding information for the DB Alias.

  Each box indicates a DBMS type and a connection string, separated by a dash. For Informix, Sybase ASE, and MS SQL Server, the connection string is followed by the database name. (The letters NA following an Informix database type indicate a Non-ANSI database.)



Command Buttons

The most common command buttons include:

Previous Return to the previous dialog. This button is not present in every dialog.

Proceed Perform any tasks initiated by the current dialog using the information provided, close the dialog, and open the next dialog in sequence.

Skip Skip one or more logically related dialogs or tasks. This button is not present in every dialog and is sometimes unavailable.

Undo Restore the dialog to its initial status. This button is not present in every dialog.

Cancel Close the current dialog and return control to the Configuration main window. This button is present in every dialog.

DBMS Terms

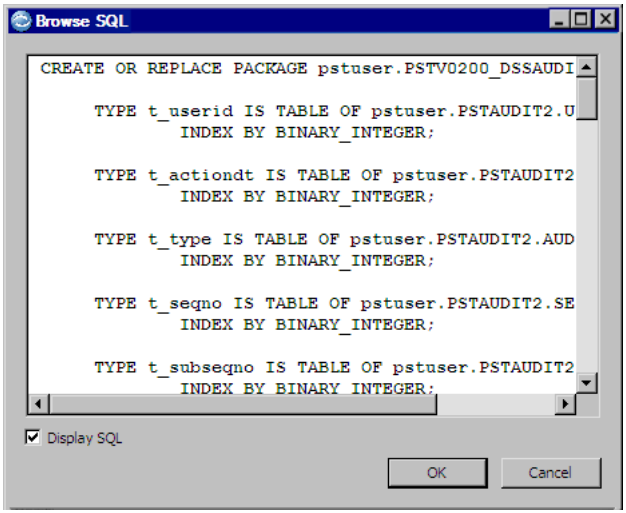
Optim supports several database management systems. Terms used in a configuration dialog reflect the DBMS for the database that is being configured. For example, when configuring an Oracle database, a configuration dialog refers to *Packages* to access database tables. However, when configuring a Sybase ASE or SQL Server database, the same dialog refers to *Procedures*, and for a DB2 database it refers to *Plans*. Varying terms are noted in the discussion of a dialog. In some instances, a particular DBMS may require a unique dialog. When this happens, both the common dialog and the DBMS-unique dialog are illustrated and discussed.

Display SQL

If the **Configuration** program creates *data definition language* statements or DDL, the pertinent dialog includes a check box, **Display SQL**. To review DDL statements before they are executed, select this check box. To execute a task without review, clear the check box.

Note: The **Configuration** program creates a text file, **sql.txt**, containing the DDL generated during the current and previous sessions. You can browse or print this file using a text editor, such as *Notepad*. The file is generated whether or not you select **Display SQL** on a particular dialog and is stored in the default Temp directory.

If you select **Display SQL** and click **Proceed**, the **Browse SQL** dialog opens, as illustrated in the following figure.



The **Browse SQL** dialog displays the generated DDL statements in sequence:

- To display the next DDL statement, select the **Display SQL** check box (may be checked when the dialog opens).
- To execute remaining DDL statements without review, clear the **Display SQL** check box.

Note: The check box to **Display SQL** is dynamic. If selected or cleared on one dialog, it automatically changes on other dialogs, where appropriate.

5. Configure Workstations

Two **Configuration** Tasks are used to configure workstations to use ***Optim***. The first, **Configure the First Workstation**, creates the ***Optim*** Directory and establishes connectivity to databases through the creation of associated DB Aliases. If additional workstations are used, the **Configure Additional Workstations** task guides you through the process needed to establish them.

Once established, any workstation can be configured as an ***Optim Server***, if your license permits.

Tasks Menu

Use the **Configuration Assistant** or commands from the **Tasks** menu to configure the ***Optim*** environment. You can choose to perform these tasks at any time.

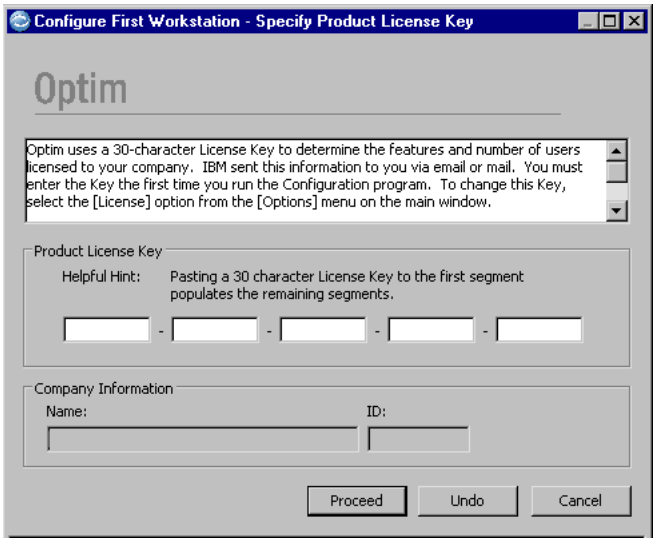
Note: Before you configure the first workstation and any additional workstations, you must sign the ***Optim*** default exit or a user-supplied exit of your own creation. You cannot continue with the Configuration process or use ***Optim*** until you sign a valid exit using the **Sign Optim Exit** dialog, as described in **Chapter 3. Signing an Optim Exit**.

5.1 Configure the First Workstation

Several steps are required to configure the first workstation. However, you need not accomplish all steps while configuring the first workstation, but can come back to them later by selecting a task directly from the **Tasks** menu. For example, you are given the opportunity to initialize and establish security when configuring the first workstation, but will probably want to perform this task sometime later. If so, you can skip this portion of the Configure the First Workstation process.

5.1.1 Specify Product License Key

The first time you start the **Configuration** program after installing ***Optim***, you are prompted to provide the Product License Key.


Configure First Workstation - Specify Product License Key
Optim
Optim uses a 30-character License Key to determine the features and number of users licensed to your company. IBM sent this information to you via email or mail. You must enter the Key the first time you run the Configuration program. To change this Key, select the [License] option from the [Options] menu on the main window.
Product License Key
Helpful Hint: Pasting a 30 character License Key to the first segment populates the remaining segments.
Company Information
Name:
ID:
Proceed
Undo
Cancel

The Product License Key provides an internal control that determines the features and number of users your company is licensed to use ***Optim***. This key may be changed from time to time when you upgrade the product. To enter the license key, you can copy it from the email sent to you by IBM. To continue, click **OK**.

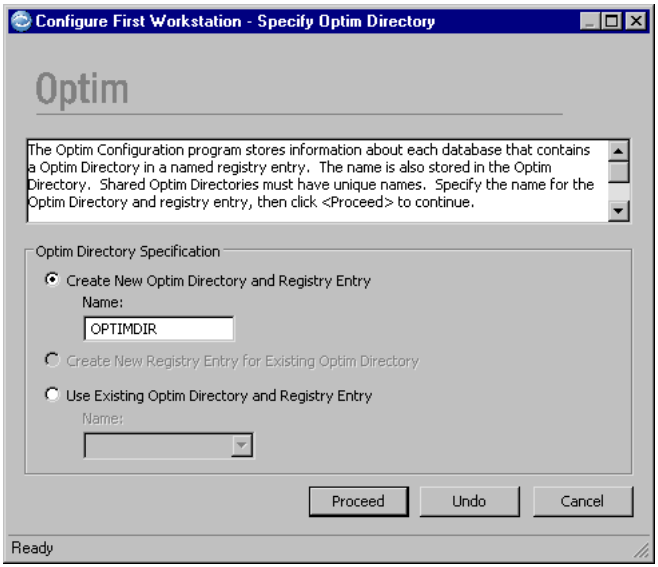
5.1.2 Create *Optim* Directory

To create an ***Optim*** Directory, you must provide the Directory name, the database instance in which the Directory resides, and the information needed to connect to the database. After creating the ***Optim*** Directory

tables, the **Configuration** program creates packages, plans, or procedures and a Windows registry entry that allows the workstation to access the ***Optim*** Directory.

Specify Optim Directory

The first step in creating an ***Optim*** Directory is to name it. Use the **Specify Optim Directory** dialog to name or select the ***Optim*** Directory.


Configure First Workstation - Specify Optim Directory
Optim
The Optim Configuration program stores information about each database that contains a Optim Directory in a named registry entry. The name is also stored in the Optim Directory. Shared Optim Directories must have unique names. Specify the name for the Optim Directory and registry entry, then click <Proceed> to continue.
Optim Directory Specification
Create New Optim Directory and Registry Entry
Name:
OPTIMDIR
Create New Registry Entry for Existing Optim Directory
Use Existing Optim Directory and Registry Entry
Name:
Proceed
Undo
Cancel
Ready

The **Specify Optim Directory** dialog presents the following options. You must select an option, enter an ***Optim*** Directory name, and click **Proceed** to open the next dialog.

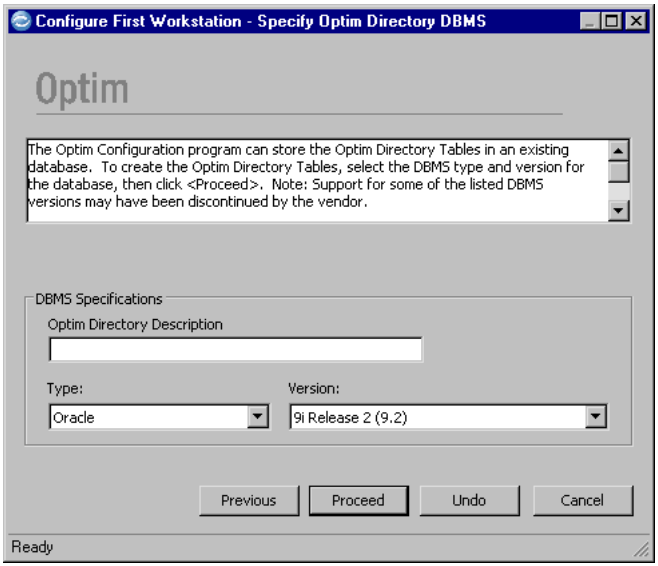
- **Create New Optim Directory and Registry Entry —** Select this option to create the first or an additional ***Optim*** Directory. This option is always available and is selected when the dialog opens.

  If no ***Optim*** Directory registry entry exists for the workstation, the default name, **OPTIMDIR**, is shown. You can use this name or enter a different name for the new ***Optim*** Directory (1 to 12 characters, no embedded blanks).

- **Use Existing Optim Directory and Registry Entry —** Select this option if you are updating or continuing the configuration of the first workstation. This option is available after an ***Optim*** Directory and Windows registry entry are created. You must enter the name of the existing ***Optim*** Directory to use.

Specify Optim Directory DBMS

Before you can create ***Optim*** Directory tables, the database instance for the ***Optim*** Directory must exist; that is, it must be configured under a database management system. To create an ***Optim*** Directory, you must identify the DBMS type and version on the **Specify Optim Directory DBMS** dialog.


Configure First Workstation - Specify Optim Directory DBMS
Optim
The Optim Configuration program can store the Optim Directory Tables in an existing database. To create the Optim Directory Tables, select the DBMS type and version for the database, then click <Proceed>. Note: Support for some of the listed DBMS versions may have been discontinued by the vendor.
DBMS Specifications
Optim Directory Description
Type:
Oracle
Version:
9i Release 2 (9.2)
Previous
Proceed
Undo
Cancel
Ready

When this dialog opens, **Optim Directory Description**, **Type**, and **Version** may be populated with previously entered information. The **Specify Optim Directory DBMS** dialog includes the following:

DBMS Specifications

Optim Directory Description

Enter text to explain the purpose of the ***Optim*** Directory (up to 40 characters). The description is especially valuable if you have multiple ***Optim*** Directories.

Type

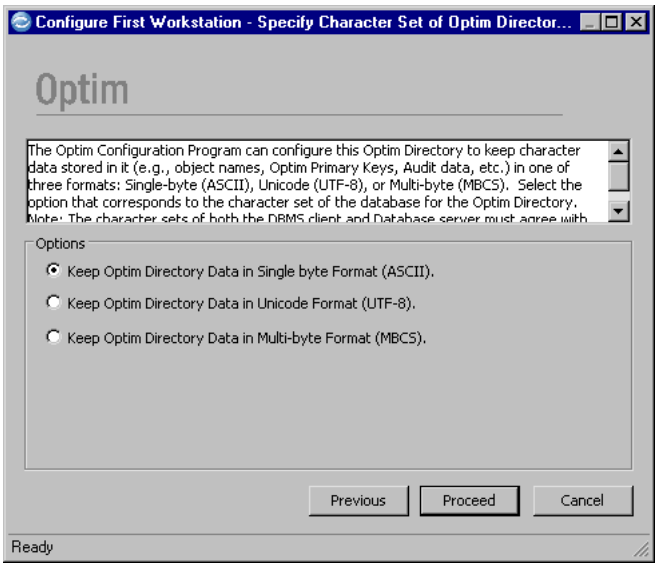
Select the DBMS for the ***Optim*** Directory database. To select from a list, click the down arrow. The selected DBMS appears on the status bar of subsequent dialogs in the process.

Note: You cannot create the ***Optim*** Directory in a DB2 z/OS database. Also, an ***Optim*** Directory in an SQL Server database is not accessible to a UNIX-based ***Optim Server***.

Version — Select the version of the DBMS for the ***Optim*** Directory database. To select from a list, click the down arrow.

Specify Character Set of Optim Directory

Character data such as object names and primary keys are stored in the ***Optim*** Directory in one of these formats: ASCII, Unicode, or multi-byte. Choose the option that corresponds to the character set of the database for the ***Optim*** Directory.


Configure First Workstation - Specify Character Set of Optim Director...
Optim
The Optim Configuration Program can configure this Optim Directory to keep character data stored in it (e.g., object names, Optim Primary Keys, Audit data, etc.) in one of three formats: Single-byte (ASCII), Unicode (UTF-8), or Multi-byte (MBCS). Select the option that corresponds to the character set of the database for the Optim Directory.
Options
Keep Optim Directory Data in Single byte Format (ASCII).
Keep Optim Directory Data in Unicode Format (UTF-8).
Keep Optim Directory Data in Multi-byte Format (MBCS).
Previous
Proceed
Cancel
Ready

The options on this dialog are:

- **Keep Optim Directory Data in Single byte Format (ASCII)**
- **Keep Optim Directory Data in Unicode Format (UTF-8)**
- **Keep Optim Directory Data in Multi-byte Format (MBCS)**

Select the option and click **Proceed** to open the next dialog.

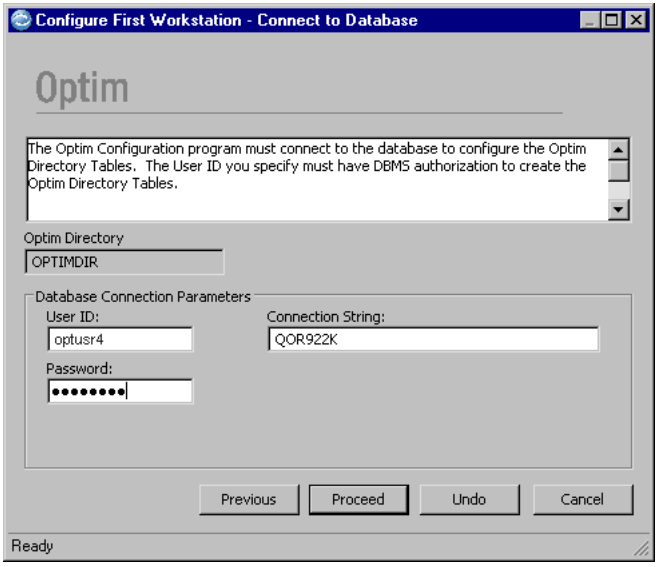
Connect to Database

The **Configuration** program must connect to the database to create the ***Optim*** Directory tables and packages, plans, or procedures. To enable this connection, you must provide a valid **User ID**, **Password**, and **Connection String**.

The User ID must have the DBMS privilege to create the tables and to catalog the packages, plans, or procedures under the appropriate table identifier (**Creator ID**, **Schema Name**, or **Owner ID**) during the

configuration process. Later, this workstation can access the ***Optim*** Directory using the same identifier or a different identifier with, perhaps, less authority.

Use the **Connect to Database** dialog to provide the connection information that allows the **Configuration** program to connect to the database and then configure ***Optim*** Directory tables.



The **Connect to Database** dialog prompts for the following Database Connection Parameters:

Optim Directory

Previously entered ***Optim*** Directory name.

Database Connection Parameters

User ID

Enter a User ID (up to 30 characters) that the DBMS requires to allow access to the ***Optim*** Directory database instance.

Password

Enter a password (up to 30 characters) that corresponds to the specified User ID.

Connection String Enter the name or string needed to access the ***Optim*** Directory database.

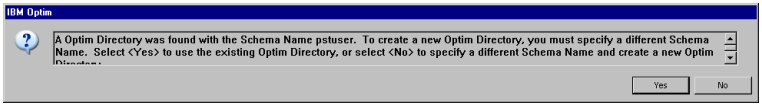
Note: If you are using DB2, the term is *Database Name* or *Alias*. Oracle uses *DB Alias*, Sybase ASE uses *Server Name*, SQL Server uses *System Data Source Name*, and Informix uses *Host Name*. Syntax is described in the DBMS documentation.

DB Name Enter the name of the Sybase ASE, SQL Server, or Informix database instance for the ***Optim*** Directory.

Note: This prompt is displayed only if the ***Optim*** Directory is in a Sybase ASE, SQL Server, or Informix database.

Note: If you are creating a new ***Optim*** Directory and specify a User ID associated with another Directory in the database, the following pop-up dialog informs you that another ID must be specified for the ***Optim*** Directory tables schema name.

- Select **Yes** to use the existing Directory instead of creating a new Directory and proceed to the **Create/Drop Packages** dialog.
- Select **No** to continue creating a new Directory and specify a new schema name in the **Create Optim Directory Tables** dialog.

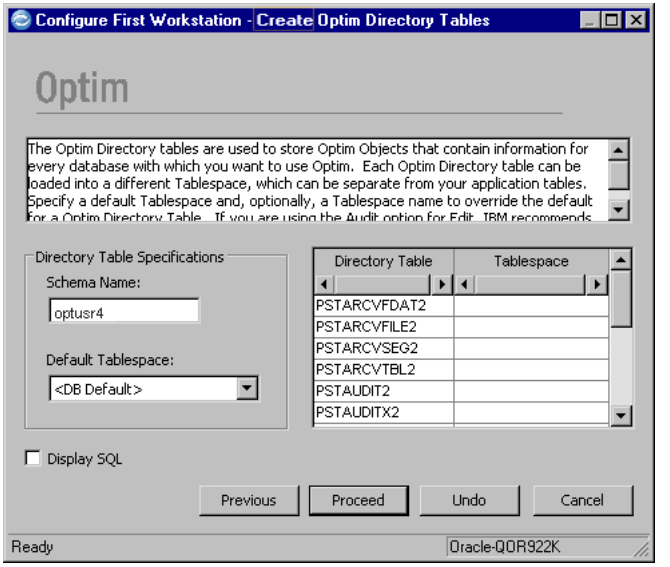

IBM Optim
A Optim Directory was found with the Schema Name pstuser. To create a new Optim Directory, you must specify a different Schema Name. Select <Yes> to use the existing Optim Directory, or select <No> to specify a different Schema Name and create a new Optim
Yes
No

Create Optim Directory Tables

After the workstation is connected to the database, you can create the ***Optim*** Directory. The **Configuration** program names the tables automatically, but you can specify the identifier (**Creator ID**, **Owner ID**, or **Schema Name**) and the database tablespace for each table.

You can create the ***Optim*** Directory tables in a unique tablespace or in the same tablespace as the other database tables. The **Create Optim Directory Tables** dialog prompts you for the information to create these tables.

You can also specify the tablespace for tables, individually or as a group, and browse the DDL generated to create the ***Optim*** Directory tables.


Configure First Workstation - Create Optim Directory Tables
Optim
The Optim Directory tables are used to store Optim Objects that contain information for every database with which you want to use Optim. Each Optim Directory table can be loaded into a different Tablespace, which can be separate from your application tables. Specify a default Tablespace and, optionally, a Tablespace name to override the default
Directory Table Specifications
Schema Name:
optusr4
Default Tablespace:
<DB Default>
Directory Table
Tablespace
PSTARCVFDAT2
PSTARCVFILE2
PSTARCVSEG2
PSTARCVTBL2
PSTAUDIT2
PSTAUDITX2
Display SQL
Previous
Proceed
Undo
Cancel
Ready
Oracle-QOR922K

The **Create Optim Directory Tables** dialog displays the following details:

Directory Table Specifications

Schema Name — Enter an identifier for the ***Optim*** Directory tables. The label is **Creator ID** when creating the ***Optim*** Directory for a DB2 database, **Schema Name** for an Oracle database, and **Owner ID** for a Microsoft SQL Server, Sybase ASE, or Informix database.

For an Oracle database, the Schema Name must not be SYS or any name that is the same as one of the ***Optim*** Directory tables (for example, PSTDBA2, PSTPK2, PSTREL2, PSTPT2).

Default Tablespace — Select a default tablespace. To select from a list of available DBMS tablespaces, click the down arrow.

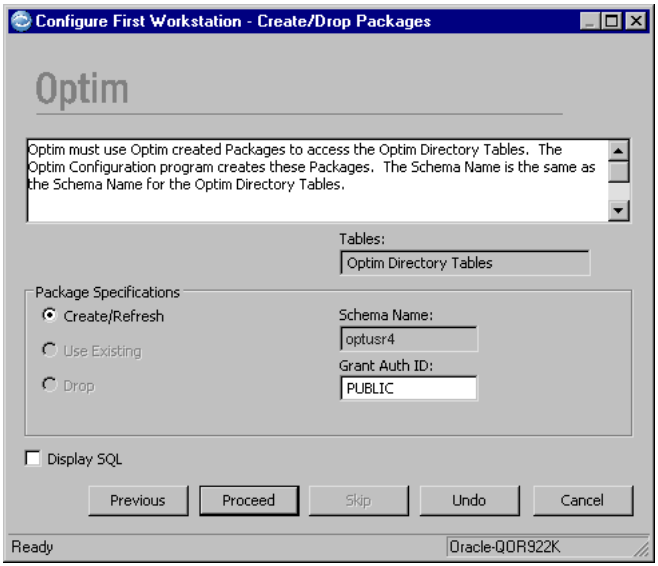
Tablespace Grid

Directory Table — The names of the ***Optim*** Directory tables.

Tablespace — Click a **Tablespace** cell to select from a list of available tablespaces in the database or leave blank to place the table in the default tablespace.

Create/Drop Packages

After the ***Optim*** Directory tables are created, the **Configuration** program automatically creates the packages, plans, or procedures used to access them. If you are creating the ***Optim*** Directory in an Oracle database the **Create/Drop Packages** dialog is displayed.



If you are using SQL Server, Sybase ASE, or Informix, the same general dialog is displayed as **Create/Drop Stored Procedures**. However, if DB2 LUW is the DBMS for the ***Optim*** Directory, the **Configuration** program displays the **Bind/Drop Plans** dialog, shown and described in **Bind/Drop Plans**.

The **Create/Drop Packages** dialog includes the following details:

Tables — Description of the tables for which packages (plans) or procedures are being created.

Package Specifications

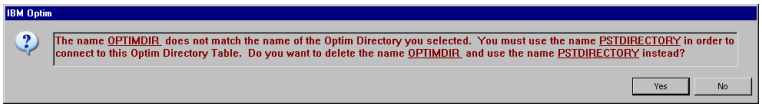
Create/Refresh — Option to create new or refresh existing ***Optim*** Directory packages (plans) or procedures. This option is always available when creating an ***Optim*** Directory and is the default selection when the dialog opens.

Use Existing	Option to use existing packages (plans) or procedures. This option is available only if packages or procedures already exist for the ***Optim*** Directory.
Drop	Option to drop existing ***Optim*** Directory packages (plans) or procedures. This option is available only if packages or procedures already exist for the ***Optim*** Directory.
Qualifier	Previously entered high-level qualifier needed to access ***Optim*** Directory tables. The label is **Collection Name** for DB2, **Schema Name** for Oracle, and **Owner ID** for SQL Server, Sybase ASE, or Informix.
Grant Auth ID	Enter an identifier for authorized users. You may specify a User ID, a Group Name, or **Public**. When this ID is Public, all users can run ***Optim***.

Display SQL Select this check box to display SQL statements before creating or dropping packages (plans) or procedures.

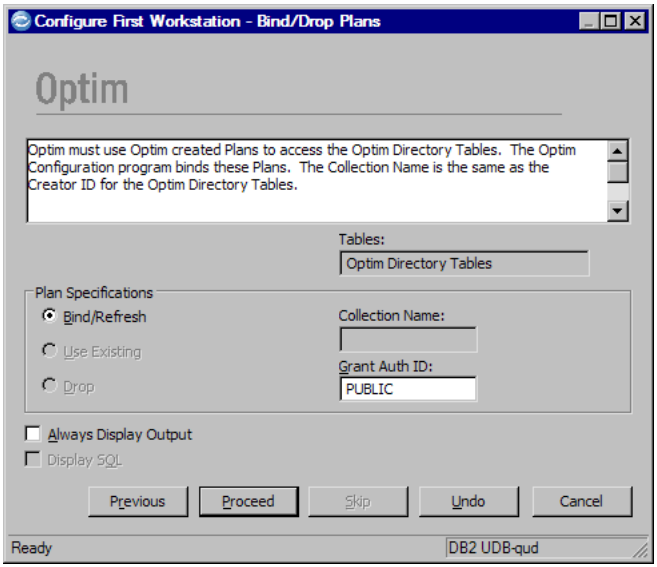
Note: If you attempted to create a new ***Optim*** Directory but responded Yes to the pop-up dialog on page 83, the following pop-up prompts you to confirm that you will use the existing Directory instead of creating a new one.

- Select **Yes** to use the existing Directory name and proceed to the **Connect to Database** dialog.
- Select **No** to not use the existing Directory name and terminate the Directory creation process.


IBM Optim
The name OPTIMDIR does not match the name of the Optim Directory you selected. You must use the name PSTDIRECTORY in order to connect to this Optim Directory Table. Do you want to delete the name OPTIMDIR and use the name PSTDIRECTORY instead?
Yes
No

Bind/Drop Plans

When creating an ***Optim*** Directory in a DB2 database, the configuration process prompts for authorization information using the **Bind/Drop Plans** dialog.



The elements in the **Bind/Drop Plans** dialog are similar to those described for **Create/Drop Packages** with the following exception:

Always Display Output Select this check box to open the **Browse File** dialog to review any errors, warnings, and information regarding the bind.

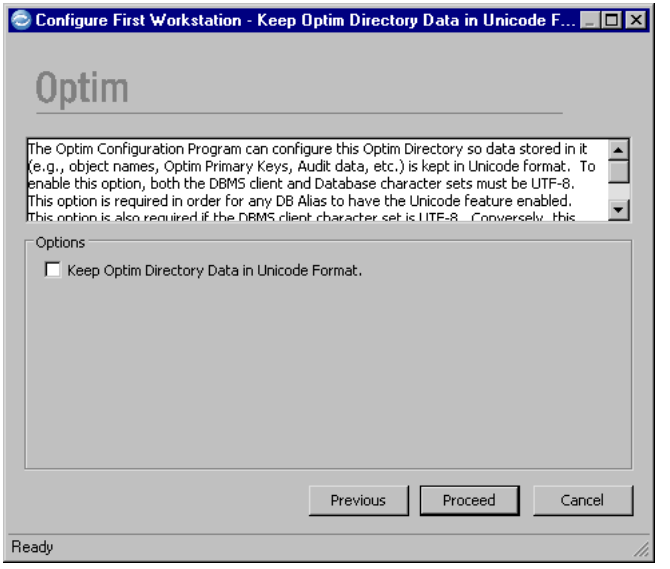
Note: If problems or a failure occurs during the bind, the **Browse File** dialog opens whether or not you select **Always Display Output**.

Define Character Format

If the ***Optim*** Directory is in a DBMS for which ***Optim*** supports Unicode (except SQL Server) or multi-byte, you must indicate the character format of the Directory.

Keep Optim Directory Data in Unicode Format

If you are creating an ***Optim*** Directory in a DBMS for which ***Optim*** supports Unicode but not multi-byte, you are prompted to indicate whether the ***Optim*** Directory data is kept in Unicode format.

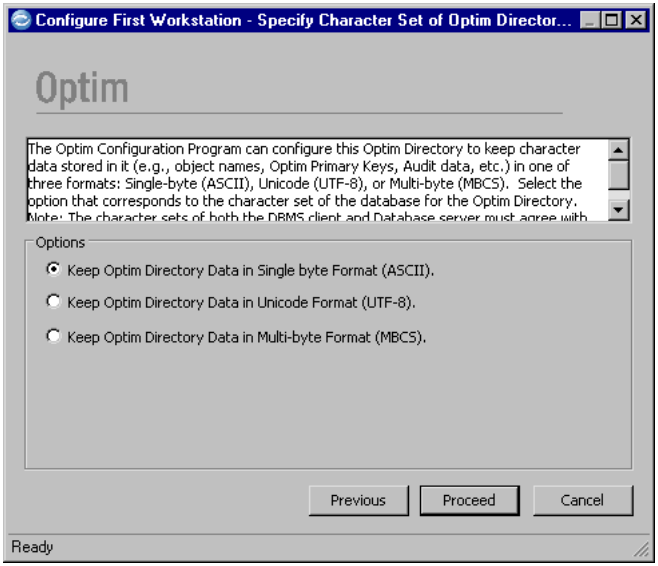

Configure First Workstation - Keep Optim Directory Data in Unicode F...
Optim
The Optim Configuration Program can configure this Optim Directory so data stored in it (e.g., object names, Optim Primary Keys, Audit data, etc.) is kept in Unicode format. To enable this option, both the DBMS client and Database character sets must be UTF-8. This option is required in order for any DB Alias to have the Unicode feature enabled.
Options
Keep Optim Directory Data in Unicode Format.
Previous
Proceed
Cancel
Ready

Note: For DB2 LUW databases. The **Special Considerations for an Optim Directory in UDB** dialog is displayed next, indicating that DB Aliases for DB2 LUW or DB2 z/OS databases in a DB2 LUW ***Optim*** Directory must use the same character format as the Directory.

Specify Character Set of Optim Directory Data

If you are creating an ***Optim*** Directory in a DBMS for which ***Optim*** supports Unicode and multi-byte, you are prompted to indicate the format in which the Directory should store data: single-byte, Unicode, or multi-byte.

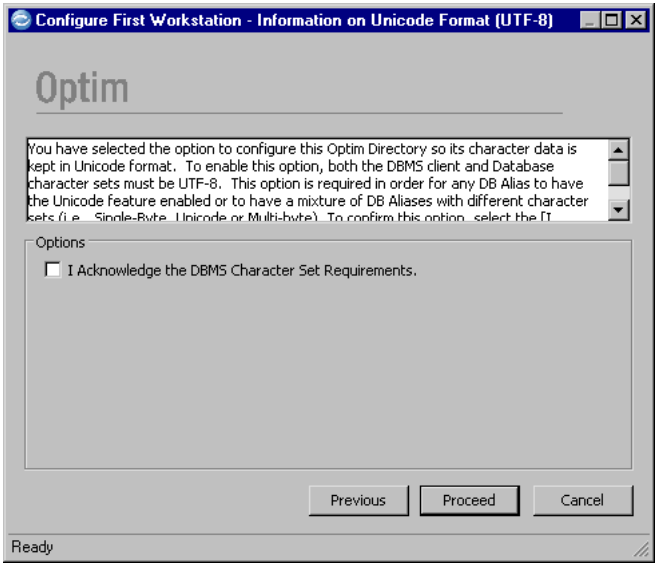
Note: The character sets of the DBMS client and the database server must match your selection.


Configure First Workstation - Specify Character Set of Optim Director...
Optim
The Optim Configuration Program can configure this Optim Directory to keep character data stored in it (e.g., object names, Optim Primary Keys, Audit data, etc.) in one of three formats: Single-byte (ASCII), Unicode (UTF-8), or Multi-byte (MBCS). Select the option that corresponds to the character set of the database for the Optim Directory.
Options
Keep Optim Directory Data in Single byte Format (ASCII).
Keep Optim Directory Data in Unicode Format (UTF-8).
Keep Optim Directory Data in Multi-byte Format (MBCS).
Previous
Proceed
Cancel
Ready

Information on Unicode Format (UTF-8)

If you select Unicode format in the **Specify Character Set of Optim Directory Data** dialog, you are prompted to acknowledge the following DBMS character set requirements for Unicode:

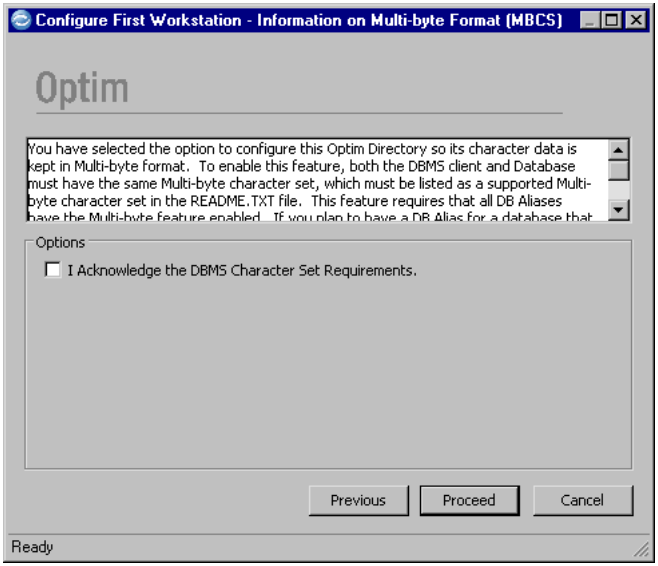
- Both the DBMS client and database character sets must be Unicode.
- The ***Optim*** Directory must be in Unicode format if it includes DB Aliases for databases of different character sets (a combination of single-byte, Unicode, or multi-byte).


Configure First Workstation - Information on Unicode Format (UTF-8)
Optim
You have selected the option to configure this Optim Directory so its character data is kept in Unicode format. To enable this option, both the DBMS client and Database character sets must be UTF-8. This option is required in order for any DB Alias to have the Unicode feature enabled or to have a mixture of DB Aliases with different character
Options
I Acknowledge the DBMS Character Set Requirements.
Previous
Proceed
Cancel
Ready

Information on Multi-byte Format (MBCS)

If you select multi-byte format in the **Specify Character Set of Optim Directory Data** dialog, you are prompted to acknowledge the following DBMS character set requirements for multi-byte:

- Both the DBMS client and database must have the same supported multi-byte character set.
- An ***Optim*** Directory in multi-byte format supports multi-byte DB Aliases only.


Configure First Workstation - Information on Multi-byte Format (MBCS)
Optim
You have selected the option to configure this Optim Directory so its character data is kept in Multi-byte format. To enable this feature, both the DBMS client and Database must have the same Multi-byte character set, which must be listed as a supported Multi-byte character set in the README.TXT file. This feature requires that all DB Aliases
Options
I Acknowledge the DBMS Character Set Requirements.
Previous
Proceed
Cancel
Ready

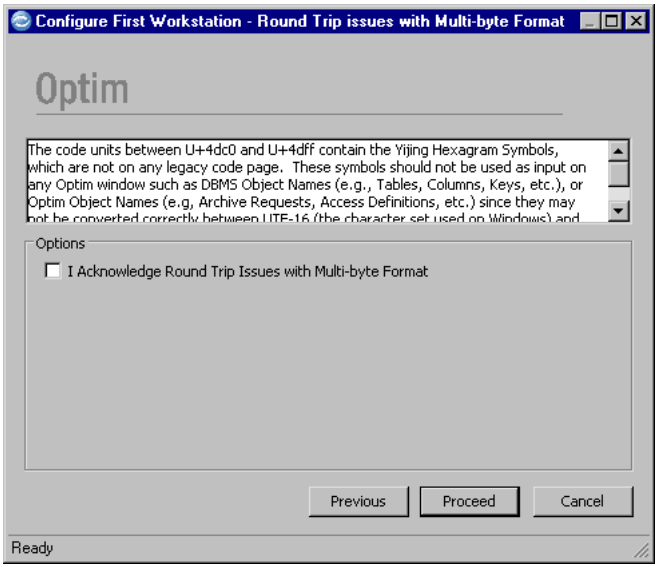
Round Trip Issues with Multi-byte Format

After you acknowledge the DBMS character set requirements for an ***Optim*** Directory in multi-byte format, you are prompted to acknowledge multi-byte round trip conversion issues.

Optim uses the Unicode character set in dialogs and to process data. In some multi-byte character sets (such as Oracle JA16SJIS), multiple characters are mapped to the same Unicode character. When these characters are converted from Unicode back to multi-byte (a round trip), the original character may not be returned.

Note: To avoid round-trip issues with multi-byte data, do not use multi-byte characters in your source data that will result in ambiguous conversions from Unicode.

Optim provides a Product Option (on the **Database** tab) and a Personal Option (on the **Database** tab) that determine how to handle round trip conversion issues when processing data in a multi-byte database.

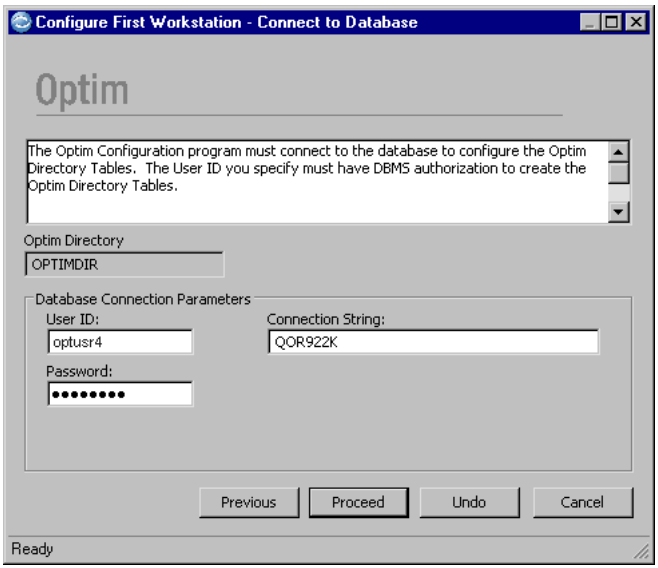

Configure First Workstation - Round Trip issues with Multi-byte Format
Optim
The code units between U+4dc0 and U+4dff contain the Yijing Hexagram Symbols, which are not on any legacy code page. These symbols should not be used as input on any Optim window such as DBMS Object Names (e.g., Tables, Columns, Keys, etc.), or Optim Object Names (e.g, Archive Requests, Access Definitions, etc.) since they may
Options
I Acknowledge Round Trip Issues with Multi-byte Format
Previous
Proceed
Cancel
Ready

Register *Optim* Directory

The **Configuration** program creates a Windows registry entry that the workstation uses to access the ***Optim*** Directory. For subsequent access to the ***Optim*** Directory from this workstation, you can use the **Connect to Database** dialog to specify a **User ID** and **Password** different from those used to create the ***Optim*** Directory. (You can modify these entries when you configure Personal Options.)

Connect to Database

The name of the ***Optim*** Directory is displayed and the **Connect to Database** dialog is populated with values entered when you created the ***Optim*** Directory.



Optim Directory

Name of the ***Optim*** Directory to which the registry entry applies.

Database Connection Parameters

User ID

Enter the User ID (up to 30 characters) that the DBMS requires to allow access to the ***Optim*** Directory database instance.

Note: For security and other reasons, it may be desirable to specify a user account with privileges that differ from those required to configure the workstation.

Password

Enter the password (up to 30 characters) that corresponds to the specified User ID.

Connection String	The name or string required to access the ***Optim*** Directory database. This value was entered earlier in the process and cannot be changed. ***Note:*** If you are using DB2, the term is *Database Name* or *Alias*. Oracle uses *DB Alias*, Sybase ASE uses *Server Name*, SQL Server uses *System Data Source Name*, and Informix uses *Host Name*. Syntax is described in the DBMS documentation.
DB Name	The name of the Sybase ASE, SQL Server, or Informix database instance for the ***Optim*** Directory. This value was entered earlier in the process and cannot be changed. ***Note:*** DB Name is displayed only if the ***Optim*** Directory is in a Sybase ASE, SQL Server, or Informix database.
Always Ask for Password	Select this check box to require a password each time you connect to the database. If you clear this check box, your password is saved in the Windows registry and you need not supply a password on future attempts to connect to the database.

This completes the process of creating the ***Optim*** Directory for the first workstation. In the next phase of the process, you create DB Aliases that allow ***Optim*** to access each database.

5.1.3 Create DB Aliases

Optim can access several databases simultaneously; however, each database must have a unique DB Alias stored in the current ***Optim*** Directory. A DB Alias is given as a high-level qualifier for a database table name to provide a single-name association for parameters required to connect to the database.

The next step in the process to configure the first workstation involves creating a DB Alias for each database and creating the packages, plans, or procedures to access tables in those databases. The **Configuration** program prompts you to:

- Create a DB Alias for the database instance housing the ***Optim*** Directory.

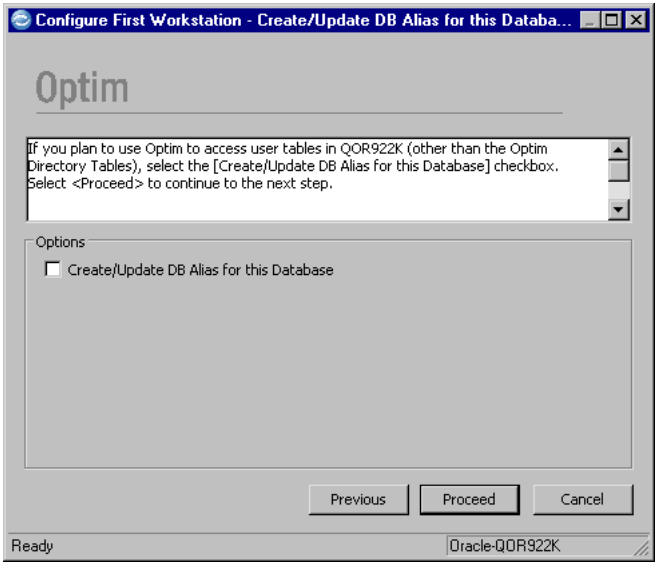
- Create ***Optim*** Primary Keys for tables that have unique indexes, if DBMS primary keys have not been created.
- Create and load the sample tables, if desired.
- Create and load the data privacy data tables, if you have an ***Optim*** Data Privacy License.

The **Configuration** program then provides an option to create DB Aliases for other databases and repeats the process.

If you have several SQL Server, Sybase ASE, or Informix databases on one server, you can use the **Create Multiple** option to create a DB Alias for each database on the server, from a single dialog.

Create DB Alias?

After you create the ***Optim*** Directory, you are prompted to create a DB Alias for the database in which it resides.


Configure First Workstation - Create/Update DB Alias for this Databa...
Optim
If you plan to use Optim to access user tables in QOR922K (other than the Optim Directory Tables), select the [Create/Update DB Alias for this Database] checkbox. Select <Proceed> to continue to the next step.
Options
Create/Update DB Alias for this Database
Previous
Proceed
Cancel
Ready
Oracle-QOR922K

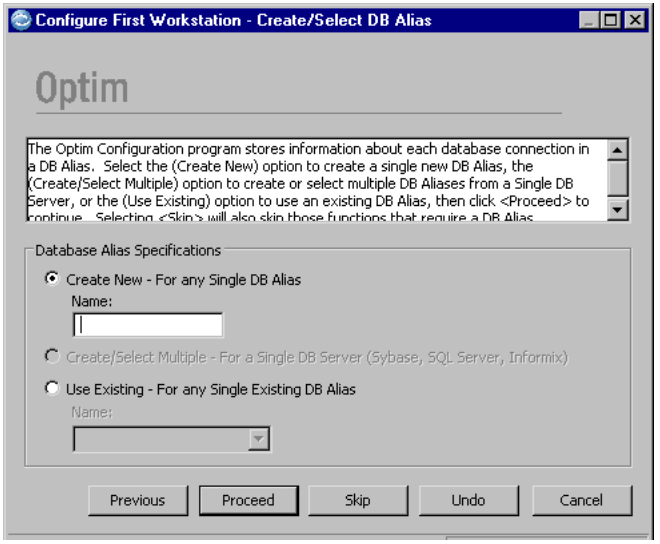
If you plan to access tables (in addition to ***Optim*** Directory tables) in the same database, select the check box to **Create/Select DB Alias for this Database**. (After creating the DB Alias you are prompted to share connection information for the DB Alias and the ***Optim*** Directory.) If you want to create a DB Alias for a different database, clear the check box.

Click **Proceed** to continue.

Create/Select DB Alias

Use the **Create/Select DB Alias** dialog to create and name a single new DB Alias, create multiple new DB Aliases for a single server, or modify an existing DB Alias.

Note: If configuring a workstation that is to function as an ***Optim Server*** (***Server***), you also must provide information for each DB Alias on the **Connections** tab on the **Optim Server Settings** applet. Refer to **6.4 Connection Tab** on page 160.


Configure First Workstation - Create/Select DB Alias
Optim
The Optim Configuration program stores information about each database connection in a DB Alias. Select the (Create New) option to create a single new DB Alias, the (Create/Select Multiple) option to create or select multiple DB Aliases from a Single DB Server, or the (Use Existing) option to use an existing DB Alias, then click <Proceed> to
Database Alias Specifications
Create New - For any Single DB Alias
Name:
Create/Select Multiple - For a Single DB Server (Sybase, SQL Server, Informix)
Use Existing - For any Single Existing DB Alias
Name:
Previous
Proceed
Skip
Undo
Cancel

The **Create/Select DB Alias** dialog presents the following options:

DB Alias Specifications

Create New — Select this option to create a new DB Alias. You must provide a name for the DB Alias.

- **Name** — Enter the name of the new DB Alias (1 to 12 characters, no embedded blanks). **Name** is blank when the **Create/Select DB Alias** dialog opens.

Create/Select Multiple — Select this option to create or select a DB Alias for each of two or more database instances on a Sybase ASE, SQL Server, or Informix database server. (Refer to **Create Multiple DB Aliases**.)

Use Existing — Select this option to use a previously created DB Alias. Use this option to modify the name of a stored procedure for an existing DB Alias.

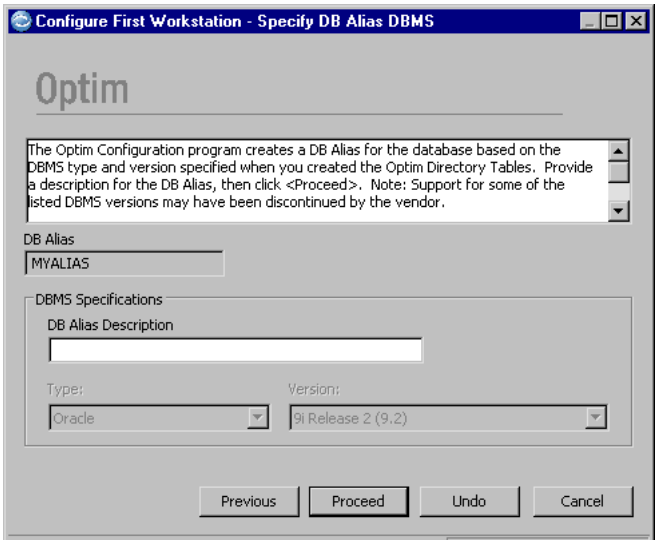
Name Select the name of the DB Alias. **Name** is available only if **Use Existing** is selected. To select from a list, click the down arrow.

Create New or Use Existing

When you select an option to create a new or modify an existing DB Alias, you are prompted for the necessary information.

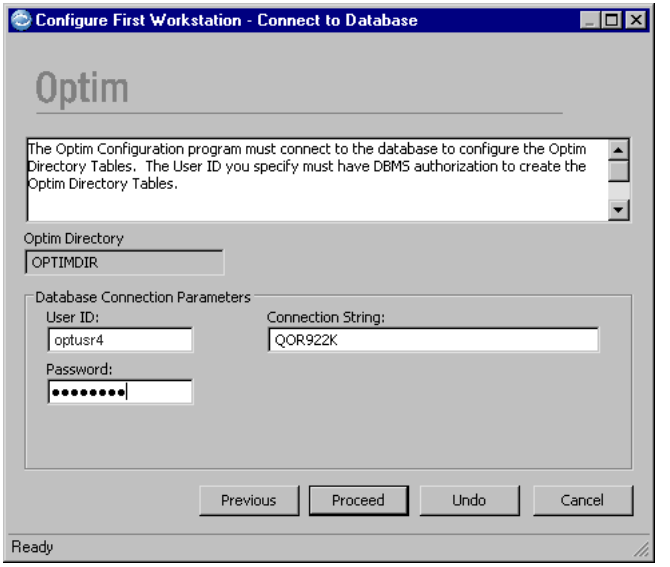
Specify DB Alias DBMS

You can provide a description to distinguish a new DB Alias from other DB Aliases. The configuration process displays the **Specify DB Alias DBMS** dialog.


Configure First Workstation - Specify DB Alias DBMS
Optim
The Optim Configuration program creates a DB Alias for the database based on the DBMS type and version specified when you created the Optim Directory Tables. Provide a description for the DB Alias, then click <Proceed>. Note: Support for some of the listed DBMS versions may have been discontinued by the vendor.
DB Alias
MYALIAS
DBMS Specifications
DB Alias Description
Type:
Oracle
Version:
9i Release 2 (9.2)
Previous
Proceed
Undo
Cancel

Connect to Database

The **Configuration** program requires certain information to configure the Catalog Tables (DB2 or Informix), Data Dictionary (Oracle), or System Tables (Microsoft SQL Server or Sybase ASE). You provide these details on the **Connect to Database** dialog.



The **Database Connection Parameters** are populated with previously entered values. Modify these values, as needed.

DB Alias

Name of the DB Alias you are creating.

Database Connection Parameters

User ID — Enter the User ID (up to 30 characters) that the DBMS requires to allow access to the ***Optim*** Directory database instance.

Password — Enter the password (up to 30 characters) that corresponds to the specified User ID.

Connection String — Enter the name or string required to access the database.

Note: If you are using DB2, the term is *Database Name* or *Alias*. Oracle uses *DB Alias*, Sybase ASE uses *Server Name*, SQL Server uses *System Data Source Name*, and Informix uses *Host Name*. Syntax is described in the DBMS documentation.

DB Name Enter the name of the Sybase ASE, SQL Server, or Informix database instance referenced by the DB Alias.

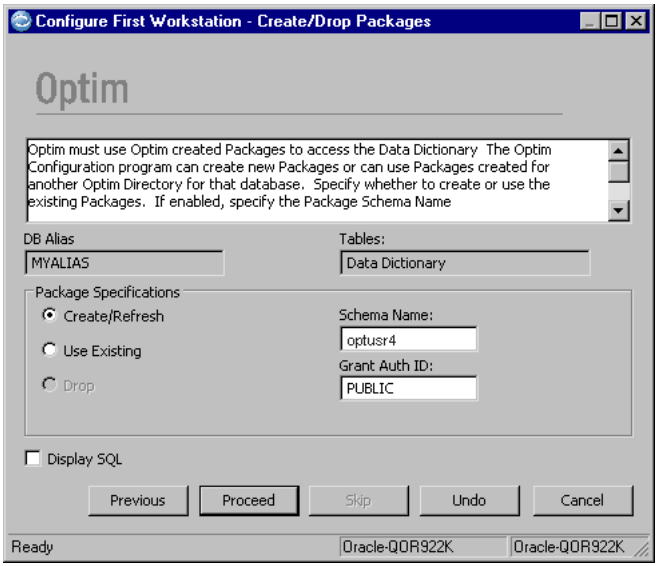
Note: This prompt is displayed only if the ***Optim*** Directory is in a Sybase ASE, SQL Server, or Informix database.

Create/Drop Packages

Access to database tables requires plans, packages, or procedures, which the configuration process creates automatically:

- If you are configuring a DB2 database, the **Bind/Drop Plans** dialog is displayed (see **Bind/Drop Plans** on page 87).
- If you are using Oracle, the **Create/Drop Packages** dialog opens. Similarly, the **Create/Drop Stored Procedures** dialog is shown for SQL Server, Sybase ASE, and Informix.

Use the **Create/Drop Packages** dialog or the **Create/Drop Stored Procedures** dialog to specify the identifier for new or existing packages (plans) or procedures, when available. You can use common stored procedures for Sybase ASE.



The **Create/Drop Packages** dialog includes the following:

DB Alias

The previously entered name for the DB Alias for which packages (plans) or procedures are being created.

Tables

Type of tables (Data Dictionary, Catalog Tables, or System Tables, depending upon the DBMS) for which packages (plans) or procedures are being created.

Stored Procedure Specifications

Create/Refresh Select this option to create new or refresh existing packages, plans, or procedures. This option is always available when creating a new DB Alias and is the default selection when the dialog opens.

Use Existing Select this option to use existing packages (plans) or procedures. The **Configuration** program creates a DB Alias that refers to the packages, plans, or procedures, but does not verify that they exist.

Drop Drop existing packages (plans) or procedures. This option is available only if packages (plans) or procedures already exist and can be dropped.

Qualifier/Prefix When enabled, enter the high-level qualifier for packages (plans) or procedures. Refers to **Collection Name** to access DB2 Catalog Tables, **Schema Name** to access the Oracle Data Dictionary, and **Owner ID** to access System Tables in SQL Server or Sybase ASE, or Informix.

Note: For Sybase ASE and SQL Server, the "sp_" prefix is displayed when stored procedures are shared and **Use One Copy for all Databases on this Server** is selected.

Grant Auth ID Enter an identifier for authorized users. You can specify a single User ID, a Group Name, or **Public**.

Use One Copy for all Databases on this Server

This check box is displayed for Sybase ASE and SQL Server only. Select the check box to use common stored procedures for databases on a single server. For Sybase ASE, stored procedures are stored in the special Sybase ASE database sybsysprocs. For SQL Server, stored procedures are stored in the MASTER database.

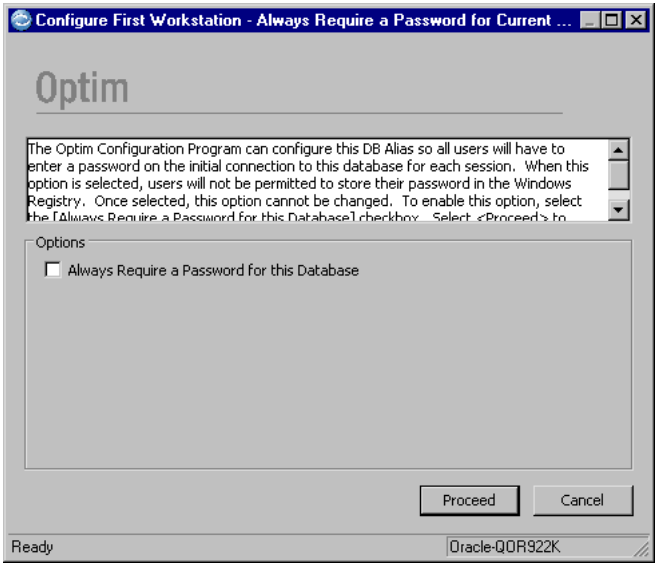
Note: Microsoft SQL Server documentation includes a caution regarding the creation of stored procedures in the MASTER database. Consider the implications of sharing stored procedures for SQL Server before proceeding.

Display SQL

Select this check box to display SQL statements before creating or dropping packages (plans) or procedures.

Always Require a Password

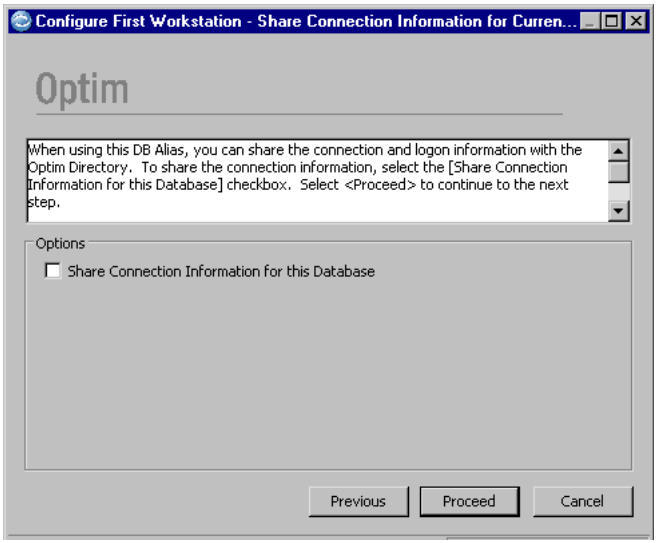
You can choose to require a password on the initial connection to the database for each session.


Configure First Workstation - Always Require a Password for Current ...
Optim
The Optim Configuration Program can configure this DB Alias so all users will have to enter a password on the initial connection to this database for each session. When this option is selected, users will not be permitted to store their password in the Windows Registry. Once selected, this option cannot be changed. To enable this option, select
Options
Always Require a Password for this Database
Proceed
Cancel
Ready
Oracle-QOR922K

If you select this option, a user of ***Optim*** must provide a password at the beginning of each session. Once you select this option, you cannot change it. To continue, click **Proceed**.

Share Connection Information

If you wish to conserve the number of database connections and the new DB Alias represents the database in which the ***Optim*** Directory resides, you may want to use only one connection for accessing both the ***Optim*** Directory and the data in the database. For this reason, the **Configuration** program displays the **Share Connection Information for Current Database** dialog after creating the packages, plans, or procedures.


Configure First Workstation - Share Connection Information for Curren...
Optim
When using this DB Alias, you can share the connection and logon information with the Optim Directory. To share the connection information, select the [Share Connection Information for this Database] checkbox. Select <Proceed> to continue to the next step.
Options
Share Connection Information for this Database
Previous
Proceed
Cancel

To access the ***Optim*** Directory and the DB Alias using a single connection, select the check box. If you clear the check box, the **Connect to Database** dialog opens and you can specify a **User ID** and **Password** for the new DB Alias.

Note: If the connection is shared, a change to the stored procedures (e.g., dropping the stored procedures or failing to perform maintenance after an installation) may prevent your connecting to the ***Optim*** Directory.

Define Character Format

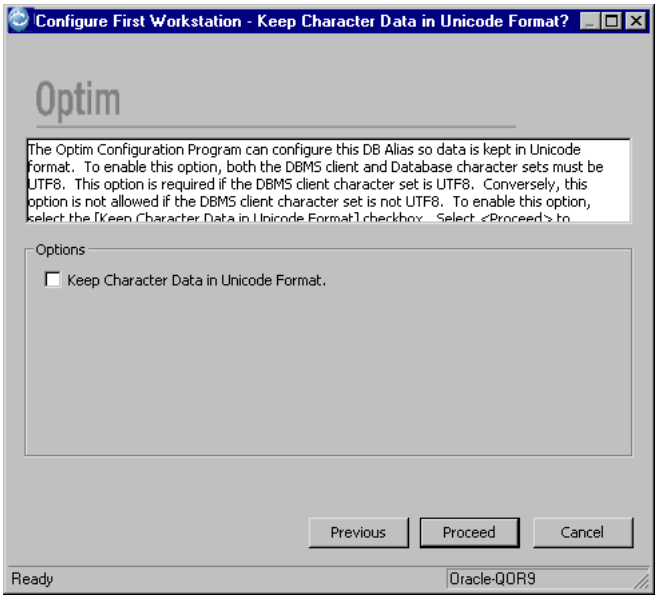
If the ***Optim*** Directory is in Unicode format and you are creating a DB Alias for a DBMS for which ***Optim*** supports Unicode (except SQL Server) or multi-byte, you must indicate the character format of the DB Alias. If the DB Alias uses a single connection with the ***Optim*** Directory, the ***Optim*** Directory and DB Alias must use the same character format.

An ***Optim*** Directory in multi-byte format supports multi-byte DB Aliases only. If the Directory is multi-byte, the DB Alias will be set to multi-byte format; however, you must respond to the **Round Trip Issues with Multi-byte Format (MBCS) for a DBA** dialog on page 107.

Note: If the DB Alias represents the database in which the ***Optim*** Directory resides, the **Keep Character Data in Unicode Format** and **Specify Character Set of DB Alias Data** dialogs are displayed after the **Share Connection Information for the Current Database** dialog. Read **Share Connection Information**.

Keep Character Data in Unicode Format

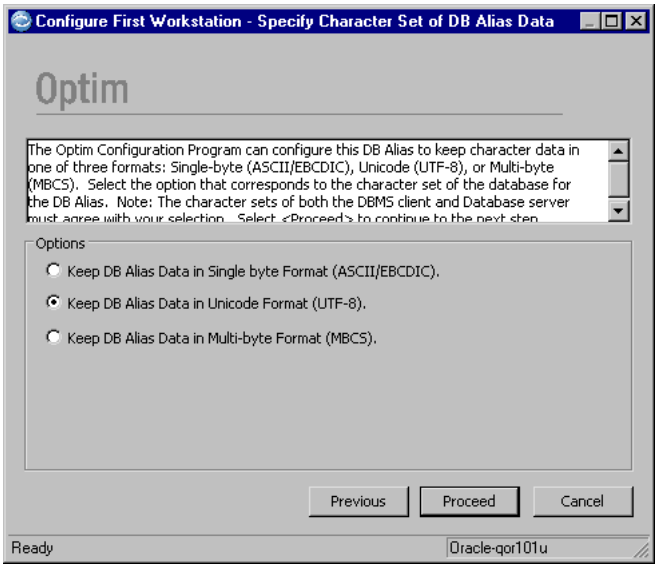
If you are creating an ***Optim*** Directory in a DBMS for which ***Optim*** supports Unicode but not multi-byte, you are prompted to indicate whether the DB Alias data is kept in Unicode format.


Configure First Workstation - Keep Character Data in Unicode Format?
Optim
The Optim Configuration Program can configure this DB Alias so data is kept in Unicode format. To enable this option, both the DBMS client and Database character sets must be UTF8. This option is required if the DBMS client character set is UTF8. Conversely, this option is not allowed if the DBMS client character set is not UTF8. To enable this option,
Options
Keep Character Data in Unicode Format.
Previous
Proceed
Cancel
Ready
Oracle-QOR9

Specify Character Set of DB Alias Data

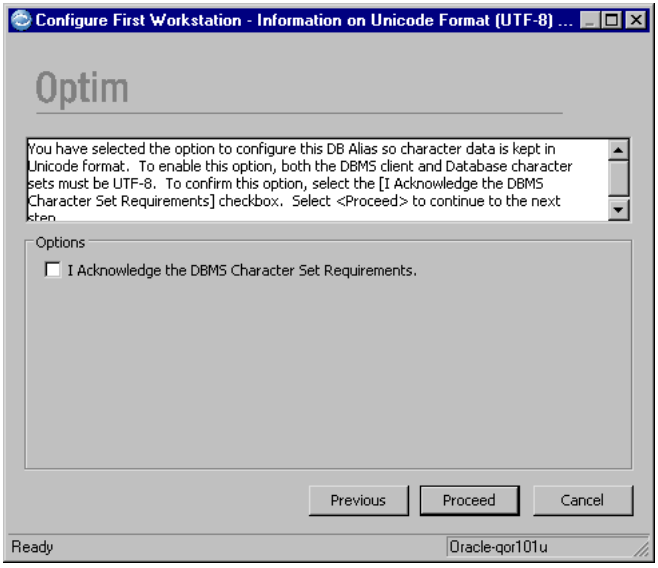
If ***Optim*** supports Unicode and multi-byte for the DB Alias DBMS, you are prompted to indicate the format in which the DB Alias should store data: single-byte, Unicode, or multi-byte.

Note: The character sets of the DBMS client and the database server must match your selection.


Configure First Workstation - Specify Character Set of DB Alias Data
Optim
The Optim Configuration Program can configure this DB Alias to keep character data in one of three formats: Single-byte (ASCII/EBCDIC), Unicode (UTF-8), or Multi-byte (MBCS). Select the option that corresponds to the character set of the database for the DB Alias. Note: The character sets of both the DBMS client and Database server must agree with your selection. Select <Proceed> to continue to the next step.
Options
Keep DB Alias Data in Single byte Format (ASCII/EBCDIC).
Keep DB Alias Data in Unicode Format (UTF-8).
Keep DB Alias Data in Multi-byte Format (MBCS).
Previous
Proceed
Cancel
Ready
Oracle-qor101u

Information on Unicode Format (UTF-8)

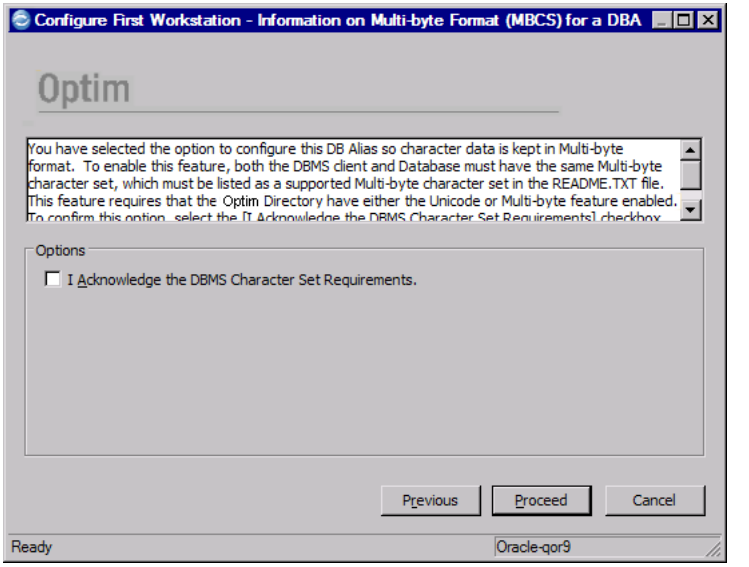
If you select Unicode format in the **Specify Character Set of DB Alias Data** dialog, you are prompted to acknowledge that the DBMS client and database character sets must be Unicode.


Configure First Workstation - Information on Unicode Format (UTF-8) ...
Optim
You have selected the option to configure this DB Alias so character data is kept in Unicode format. To enable this option, both the DBMS client and Database character sets must be UTF-8. To confirm this option, select the [I Acknowledge the DBMS Character Set Requirements] checkbox. Select <Proceed> to continue to the next
Options
I Acknowledge the DBMS Character Set Requirements.
Previous
Proceed
Cancel
Ready
Oracle-qor101u

Information on Multi-byte Format (MBCS) for a DBA

If you select multi-byte format in the **Specify Character Set of DB Alias Data** dialog, you are prompted to acknowledge the following DBMS character set requirements for multi-byte:

- Both the DBMS client and database must have the same supported multi-byte character set.
- The ***Optim*** Directory must be in Unicode or multi-byte format.


Configure First Workstation - Information on Multi-byte Format (MBCS) for a DBA
Optim
You have selected the option to configure this DB Alias so character data is kept in Multi-byte format. To enable this feature, both the DBMS client and Database must have the same Multi-byte character set, which must be listed as a supported Multi-byte character set in the README.TXT file. This feature requires that the Optim Directory have either the Unicode or Multi-byte feature enabled.
Options
I Acknowledge the DBMS Character Set Requirements.
Previous
Proceed
Cancel
Ready
Oracle-qor9

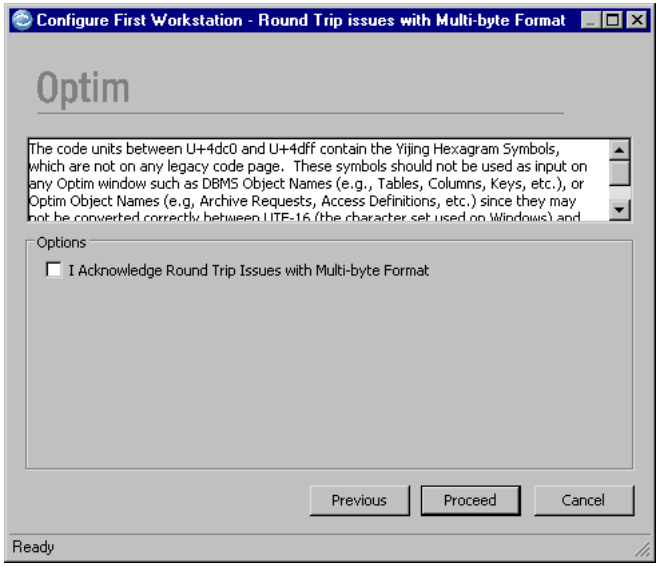
Round Trip Issues with Multi-byte Format for a DBA

After you acknowledge the DBMS character set requirements for a DB Alias in multi-byte format, or if the ***Optim*** Directory is in multi-byte format, you are prompted to acknowledge multi-byte round trip conversion issues.

Optim uses the Unicode character set in dialogs and to process data. In some multi-byte character sets (such as Oracle JA16SJIS), multiple characters are mapped to the same Unicode character. When these characters are converted from Unicode back to multi-byte (a round trip), the original character may not be returned.

Note: To avoid round-trip issues with multi-byte data, do not use multi-byte characters in your source data that will result in ambiguous conversions from Unicode.

Optim provides a Product Option (on the **Database** tab) and a Personal Option (on the **Database** tab) that determine how to handle round trip conversion issues when processing data in a multi-byte database.

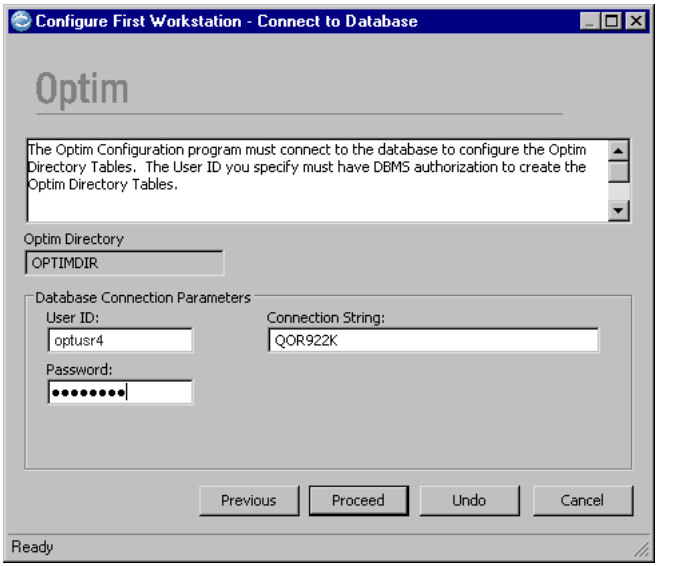

Configure First Workstation - Round Trip issues with Multi-byte Format
Optim
The code units between U+4dc0 and U+4dff contain the Yijing Hexagram Symbols, which are not on any legacy code page. These symbols should not be used as input on any Optim window such as DBMS Object Names (e.g., Tables, Columns, Keys, etc.), or Optim Object Names (e.g, Archive Requests, Access Definitions, etc.) since they may
Options
I Acknowledge Round Trip Issues with Multi-byte Format
Previous
Proceed
Cancel
Ready

Register DB Alias

The **Configuration** program creates a registry entry for subsequent access to the database. Unless the connection is shared with the ***Optim*** Directory, you must provide, on the **Connect to Database** dialog, information needed for this registry entry.

Connect to Database

When the **Connect to Database** dialog opens, **User ID**, **Password**, and **Connection String** are populated with any previously entered values.



DB Alias

Name of the DB Alias.

Database Connection Parameters

User ID

Enter the User ID (up to 30 characters) that the DBMS requires to allow access to the ***Optim*** Directory database instance.

Note: For security and other reasons, a User ID with privileges different from those required to configure the server may be desirable.

Password

Enter the password (up to 30 characters) that corresponds to the specified User ID.

Connection String

String (or name) that allows the workstation to access the ***Optim*** Directory database. The DBMS uses this connection string to recognize the database. This value was entered earlier in the process and cannot be edited.

DB Name Name that identifies the database for the DB Alias. This name is assigned when the database is created.

Note: The database name applies to Sybase ASE, SQL Server, and Informix and refers to a particular database for a given server that is referenced by the DB Alias.

Always Ask for Password Select this check box to require a password each time you connect to the database. If you clear this check box, you need not supply a password on future attempts to connect to the database.

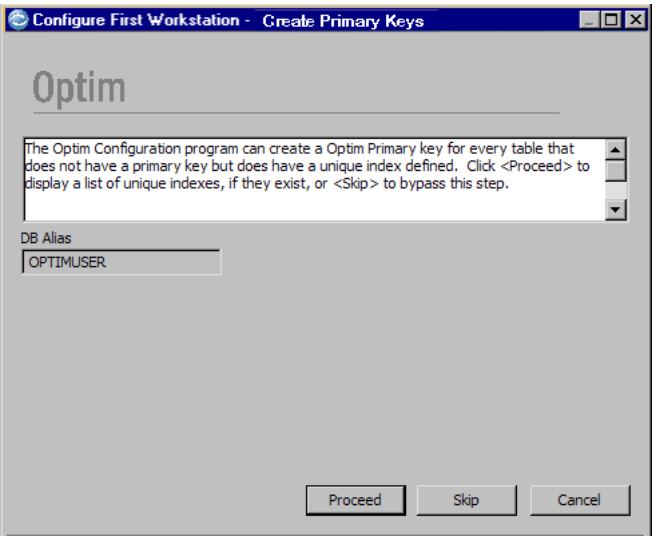
Note: This option is selected and unavailable if you selected the earlier option to **Always Require a Password for this Database**.

This completes the steps for creating the DB Aliases. Next, you create ***Optim*** Primary Keys for databases you want to use with ***Optim***.

Create Primary Keys

In some cases, primary keys are required to extract and insert data. Certain tables in the database may not have primary keys, but may have unique indexes. You can use the **Configuration** program to create ***Optim*** Primary Keys for these tables. ***Optim*** Primary Keys are stored in the ***Optim*** Directory and supplement primary keys defined to the database.

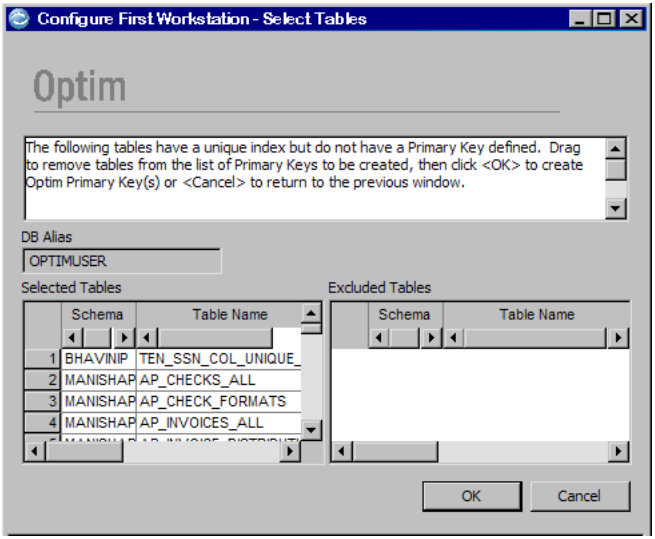
Use the **Create Primary Keys** dialog to confirm the DB Alias for the database tables that require ***Optim*** Primary Keys.


Configure First Workstation - Create Primary Keys
Optim
The Optim Configuration program can create a Optim Primary key for every table that does not have a primary key but does have a unique index defined. Click <Proceed> to display a list of unique indexes, if they exist, or <Skip> to bypass this step.
DB Alias
OPTIMUSER
Proceed
Skip
Cancel

Note: You can also create ***Optim*** Primary Keys on a table-by-table basis.

Select Tables

The **Select Tables** dialog allows you to select tables for creating ***Optim*** Primary Keys.


Configure First Workstation - Select Tables
Optim
The following tables have a unique index but do not have a Primary Key defined. Drag to remove tables from the list of Primary Keys to be created, then click <OK> to create Optim Primary Key(s) or <Cancel> to return to the previous window.
DB Alias
OPTIMUSER
Selected Tables
Schema
Table Name
1 BHAVINIP TEN_SSN_COL_UNIQUE_
2 MANISHAP AP_CHECKS_ALL
3 MANISHAP AP_CHECK_FORMATS
4 MANISHAP AP_INVOICES_ALL
Excluded Tables
Schema
Table Name
OK
Cancel

The **Select Tables** dialog includes:

DB Alias

DB Alias associated with the list of tables.

Selected Tables

List of tables selected for creating primary keys. To remove a table from the list, drag the table name to **Excluded Tables**.

Creator ID Identifier for the table. (**Creator ID** in DB2, **Schema Name** in Oracle, and **Owner ID** for SQL Server, Sybase ASE, and Informix.)

Table Name Name of the table.

Index Name Name of the unique index.

Excluded Tables

List of excluded tables available for creating primary keys. To select an excluded table, drag the table name to **Selected Tables**.

Creator ID Identifier for the table. (**Creator ID** in DB2, **Schema Name** in Oracle, and **Owner ID** for SQL Server, Sybase ASE, or Informix.)

Table Name Name of the table.

Index Name Name of the unique index.

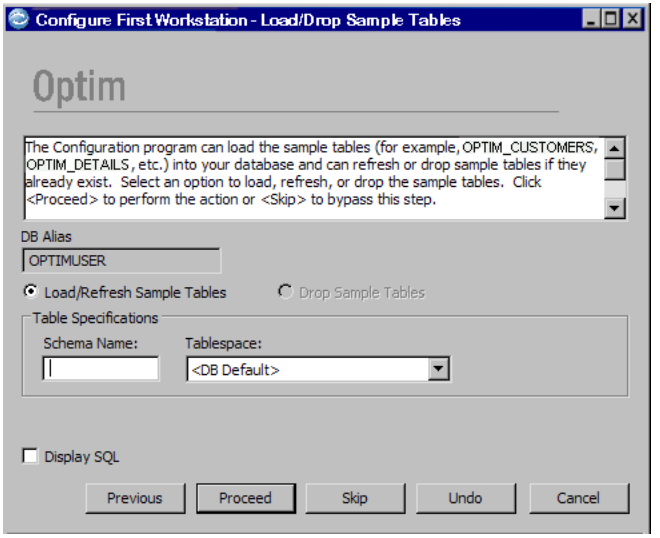
When the process completes, you are prompted to load the sample database tables.

Load Sample Tables

This software is distributed with sample data tables. You can use these tables for training and to experiment with sample data before applying the software to your own database tables. Generally, the sample data is loaded when you configure the first workstation, but you also can load or refresh that data by selecting **Load/Drop Sample Data** from the **Tasks** menu.

Load/Drop Sample Tables

The **Load/Drop Sample Tables** dialog allows you to provide the identifier (**Creator ID**, **Schema**, or **Owner ID**) and tablespace for the sample tables before they are loaded.


Configure First Workstation - Load/Drop Sample Tables
Optim
The Configuration program can load the sample tables (for example, OPTIM_CUSTOMERS, OPTIM_DETAILS, etc.) into your database and can refresh or drop sample tables if they already exist. Select an option to load, refresh, or drop the sample tables. Click <Proceed> to perform the action or <Skip> to bypass this step.
DB Alias
OPTIMUSER
Load/Refresh Sample Tables
Drop Sample Tables
Table Specifications
Schema Name:
Tablespace:
<DB Default>
Display SQL
Previous
Proceed
Skip
Undo
Cancel

The **Load/Drop Sample Tables** dialog displays the following:

DB Alias

DB Alias for sample tables. If you do not want to load sample tables for this DB Alias, click **Skip**.

Load/Refresh Sample Tables

Select this option to load or refresh sample tables. This option is available and selected when **Load/Drop Sample Table** opens.

Drop Sample Tables

Select this option to drop previously loaded sample tables. This option is unavailable when not applicable, such as when you are initially loading those tables.

Sample Table Specifications

Schema Name — Enter an identifier for the sample tables. This element is labeled **Creator ID** for DB2, **Schema Name** for Oracle, and **Owner ID** for an SQL Server, Sybase ASE, or Informix database.

Tablespace — Select a tablespace to store the tables. To select from a list, click the down arrow. Tablespace is not available if you select **Drop Sample Tables**.

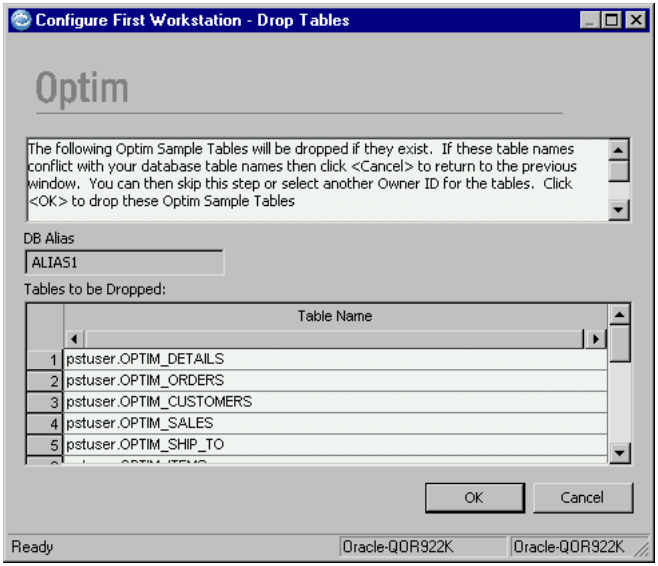
Display SQL

Select this check box to display SQL statements before loading or dropping the tables.

Note: If you are loading or refreshing the sample tables, click **Proceed** to open the **Drop Tables** dialog.

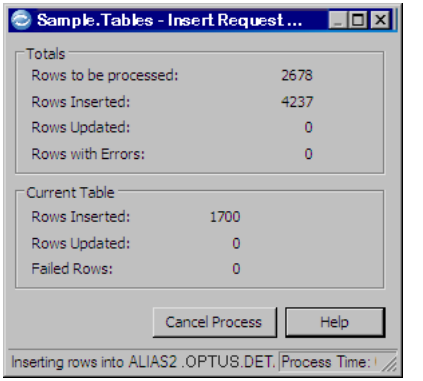
Drop Tables

The **Drop Tables** dialog allows you to review a list of the sample tables that are to be dropped within the selected DB Alias.


Configure First Workstation - Drop Tables
Optim
The following Optim Sample Tables will be dropped if they exist. If these table names conflict with your database table names then click <Cancel> to return to the previous window. You can then skip this step or select another Owner ID for the tables. Click <OK> to drop these Optim Sample Tables
DB Alias
ALIAS1
Tables to be Dropped:
Table Name
1 pstuser.OPTIM_DETAILS
2 pstuser.OPTIM_ORDERS
3 pstuser.OPTIM_CUSTOMERS
4 pstuser.OPTIM_SALES
5 pstuser.OPTIM_SHIP_TO
OK
Cancel
Ready
Oracle-QOR922K
Oracle-QOR922K

Use the **Drop Tables** dialog to ensure that the names of the sample tables do not conflict with your other table names. If there are conflicts, click **Cancel**; otherwise, click **OK**.

During the process that drops sample tables and loads/refreshes sample tables, the **Configuration** program displays the **Insert Request Progress** dialog.



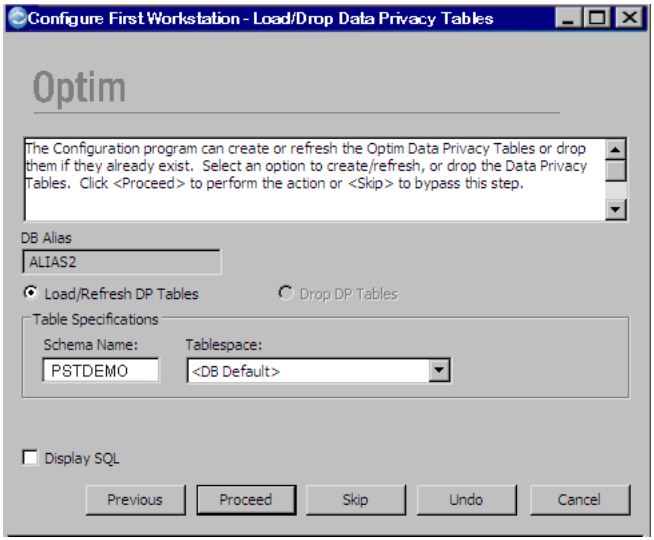
Load Data Privacy Data Tables

Data privacy data tables are available to clients who have an ***Optim*** Data Privacy License; thus, the instructions that follow apply only to those clients.

Data privacy tables allow you to mask company and personal data — such as employee names, customer names, social security numbers, credit card numbers, and e-mail addresses — to generate transformed data that is both valid and unique. Generally, these data privacy tables are loaded when you configure the first workstation, but you also can load or refresh them by selecting **Load/Drop Data Privacy Data** from the **Tasks** menu.

Load/Drop Data Privacy Tables

The **Load/Drop Data Privacy Tables** dialog allows you to provide the identifier (**Creator ID**, **Schema**, or **Owner ID**) and tablespace for the data privacy tables before they are loaded.


Configure First Workstation - Load/Drop Data Privacy Tables
Optim
The Configuration program can create or refresh the Optim Data Privacy Tables or drop them if they already exist. Select an option to create/refresh, or drop the Data Privacy Tables. Click <Proceed> to perform the action or <Skip> to bypass this step.
DB Alias
ALIAS2
Load/Refresh DP Tables
Drop DP Tables
Table Specifications
Schema Name:
Tablespace:
PSTDEMO
<DB Default>
Display SQL
Previous
Proceed
Skip
Undo
Cancel

The **Load/Drop Data Privacy Tables** dialog displays the following:

DB Alias

DB Alias for the data privacy tables. If you do not want to load data privacy tables for this DB Alias, click **Skip**.

Load/Refresh DP Tables

Select this option to load or refresh data privacy tables. This option is available and selected when **Load/Drop Data Privacy Table** opens.

Drop DP Tables

Select this option to drop previously loaded data privacy tables. This option is unavailable when not applicable, such as when you are initially loading those tables.

Table Specifications

Schema Name Enter an identifier for the data privacy tables. This element is labeled **Creator ID** for DB2, **Schema Name** for Oracle, and **Owner ID** for an SQL Server, Sybase ASE, or Informix database.

Tablespace Select a tablespace to store the tables. To select from a list, click the down arrow. Tablespace is not available if you select **Drop DP Tables**.

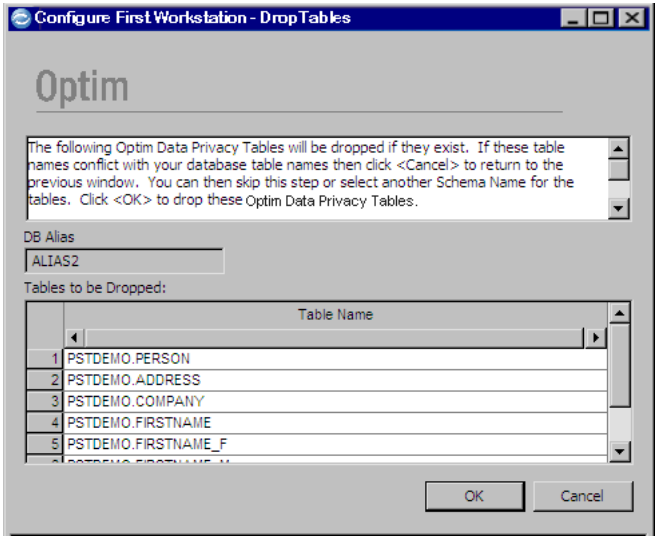
Display SQL

Select this check box to display SQL statements before creating or dropping the tables.

Note: If you are loading or refreshing the data privacy tables, click **Proceed** to open the **Drop Tables** dialog.

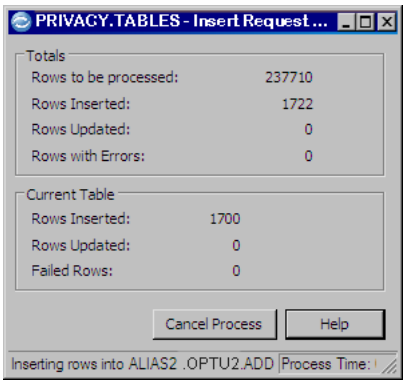
Drop Tables

The **Drop Tables** dialog allows you to review the list of the data privacy tables that are to be dropped within the selected DB Alias.


Configure First Workstation - DropTables
Optim
The following Optim Data Privacy Tables will be dropped if they exist. If these table names conflict with your database table names then click <Cancel> to return to the previous window. You can then skip this step or select another Schema Name for the tables. Click <OK> to drop these Optim Data Privacy Tables.
DB Alias
ALIAS2
Tables to be Dropped:
Table Name
1 PSTDEMO.PERSON
2 PSTDEMO.ADDRESS
3 PSTDEMO.COMPANY
4 PSTDEMO.FIRSTNAME
5 PSTDEMO.FIRSTNAME_F
OK
Cancel

Use the **Drop Tables** dialog to ensure that the names of the data privacy tables do not conflict with your other table names. If there are conflicts, click **Cancel** and specify a different schema name for the tables; otherwise, click **OK**.

During the process that drops data privacy tables and loads/refreshes tables, the **Configuration** program displays the **Insert Request Progress** dialog.



Create/Update Another DB Alias

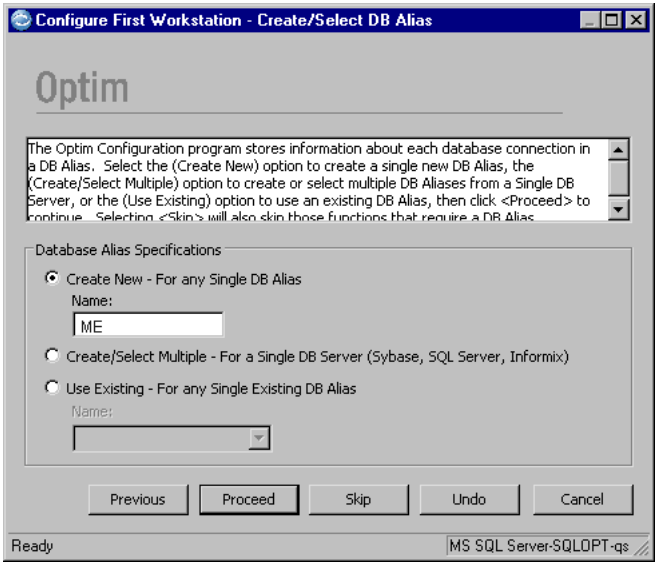
At this point, the steps for creating a new DB Alias are complete. To use ***Optim*** with additional databases, you must create corresponding DB Aliases. After you load the sample tables and the data privacy tables, the **Configuration** program prompts you to create another DB Alias. Your positive response opens the **Create/Select DB Alias** dialog to repeat the configuration process for another database.

Note: If the DB Alias you created is for a DB2 z/OS database, the **Create Copies of DB2 MVS Relationships** dialog displays, instead of the prompt to create another DB Alias. That dialog allows you to copy the DB2 relationships into the ***Optim*** Directory to reduce the run time when accessing DB2 tables, as described in **7.14 Create Copies of DB2 z/OS Relationships** on page 235. After that task is completed, the **Configuration** program will prompt you to create another DB Alias, as indicated above.

After all DB Aliases are created, you can configure Personal and Product Options. Refer to **5.1.5 Configure Options**.

Create Multiple DB Aliases

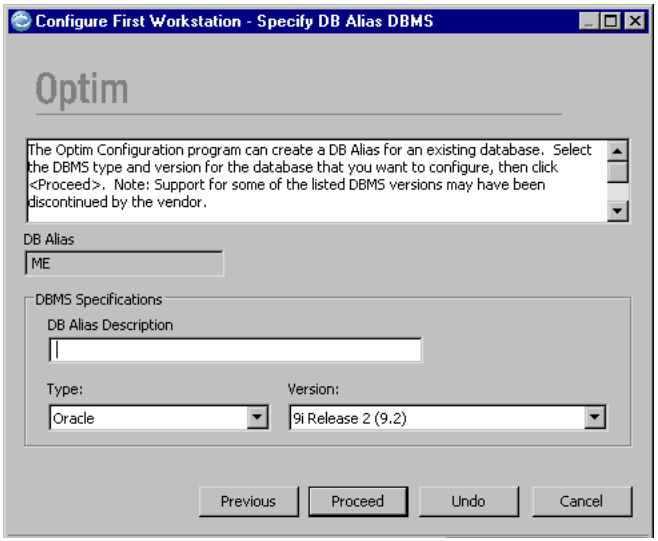
If you are using SQL Server, Sybase ASE, or Informix, you may have several databases on one server. You can create multiple DB Aliases, one for each database, in a single operation.


Configure First Workstation - Create/Select DB Alias
Optim
The Optim Configuration program stores information about each database connection in a DB Alias. Select the (Create New) option to create a single new DB Alias, the (Create/Select Multiple) option to create or select multiple DB Aliases from a Single DB Server, or the (Use Existing) option to use an existing DB Alias, then click <Proceed> to
Database Alias Specifications
Create New - For any Single DB Alias
Name:
ME
Create/Select Multiple - For a Single DB Server (Sybase, SQL Server, Informix)
Use Existing - For any Single Existing DB Alias
Name:
Previous
Proceed
Skip
Undo
Cancel
Ready
MS SQL Server-SQLOPT-qs

Although you can select the option to **Create New** and follow the steps for each database, the option to **Create/Select Multiple** saves time by allowing you to set specifications for each database at the same time.

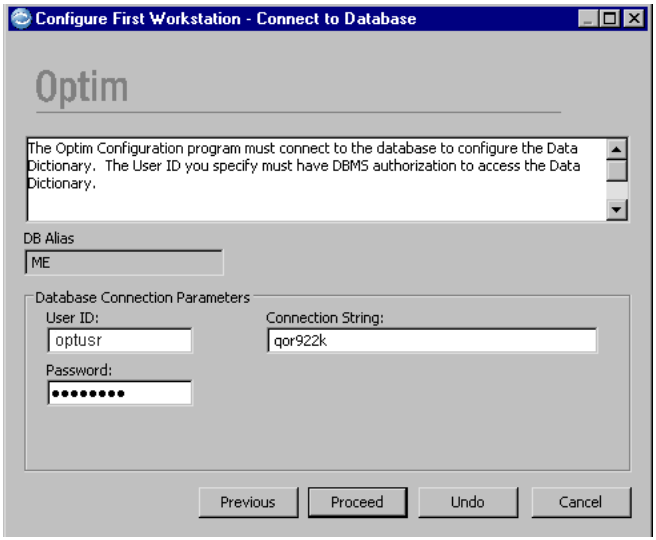
On the **Create/Select DB Alias** dialog, select the option to **Create/Select Multiple — For a Single DB Server (Sybase, SQL Server, Informix)**, and click **Proceed**.

The **Configuration** program opens the **Specify DB Alias DBMS** dialog.


Configure First Workstation - Specify DB Alias DBMS
Optim
The Optim Configuration program can create a DB Alias for an existing database. Select the DBMS type and version for the database that you want to configure, then click <Proceed>. Note: Support for some of the listed DBMS versions may have been discontinued by the vendor.
DB Alias
ME
DBMS Specifications
DB Alias Description
Type:
Oracle
Version:
9i Release 2 (9.2)
Previous
Proceed
Undo
Cancel

Select the DBMS **Type** and **Version** and click **Proceed**.

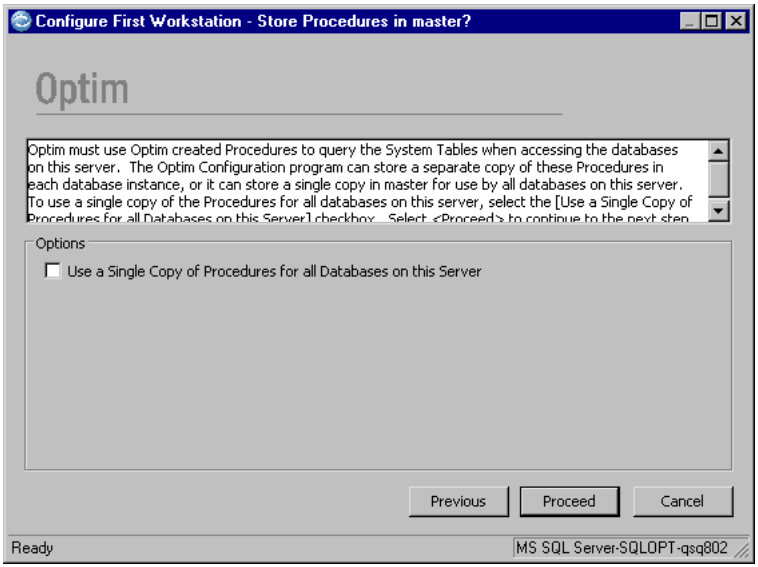
The **Connect to Database** dialog is displayed next.



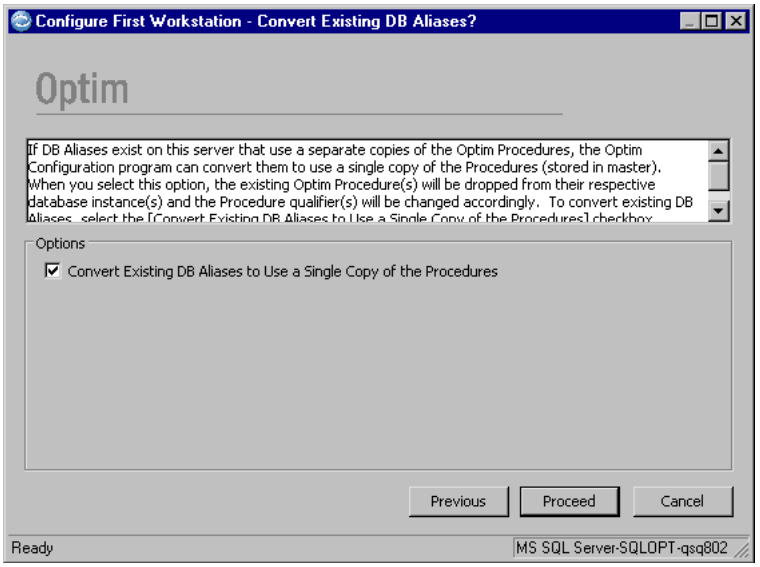
Specify a **User ID** and **Password** with authority to connect to the master database on the server, and click proceed to open the **Create Multiple DB Aliases** dialog (shown and described on page 121).

Note: For SQL Server, the User ID must have database owner (dbo) privileges to create or select multiple DB Aliases.

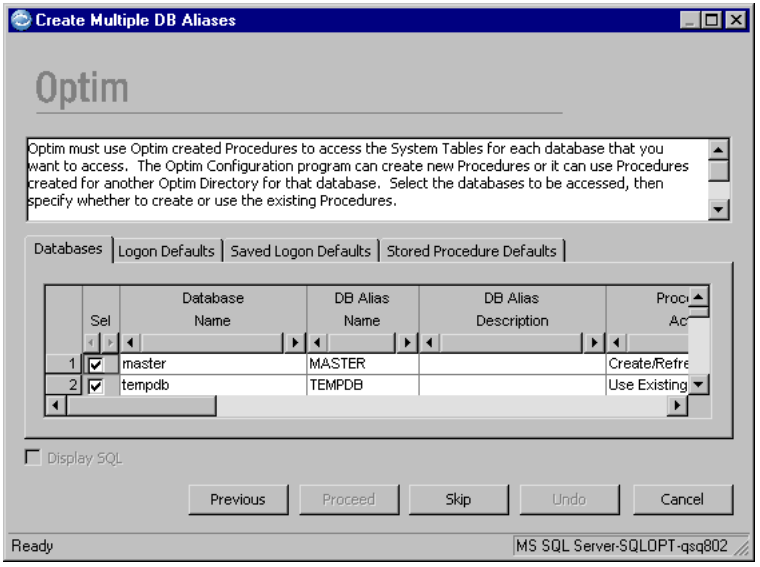
For Sybase ASE and SQL Server, you are prompted to share a single copy of the stored procedures.


Configure First Workstation - Store Procedures in master?
Optim
Optim must use Optim created Procedures to query the System Tables when accessing the databases on this server. The Optim Configuration program can store a separate copy of these Procedures in each database instance, or it can store a single copy in master for use by all databases on this server. To use a single copy of the Procedures for all databases on this server, select the [Use a Single Copy of
Options
Use a Single Copy of Procedures for all Databases on this Server
Previous
Proceed
Cancel
Ready
MS SQL Server-SQLOPT-qsq802

If you select the check box to share stored procedures, you are prompted to convert existing DB Aliases to use the shared procedures.


Configure First Workstation - Convert Existing DB Aliases?
Optim
If DB Aliases exist on this server that use a separate copies of the Optim Procedures, the Optim Configuration program can convert them to use a single copy of the Procedures (stored in master). When you select this option, the existing Optim Procedure(s) will be dropped from their respective database instance(s) and the Procedure qualifier(s) will be changed accordingly. To convert existing DB
Options
Convert Existing DB Aliases to Use a Single Copy of the Procedures
Previous
Proceed
Cancel
Ready
MS SQL Server-SQLOPT-qsq802

Click proceed to open the **Create Multiple DB Aliases** dialog and enter the database information.



The **Create Multiple DB Aliases** dialog includes the following tabs.

Databases	A list of all databases that reside on the server. Enter explicit information for each database for which you want to create a DB Alias.
Logon Defaults	Enter default **User ID** and **Password** required to create or refresh stored procedures for each DB Alias. In some cases, this logon may have greater privileges than the **Saved Logon Defaults**.
Saved Logon Defaults	Enter the **User ID** and **Password** required to access the database. This information is saved to the Windows registry for the workstation being configured.
Stored Procedure Defaults	Enter the default **Procedure Qualifier** and **Grant Authorization ID** required to create/refresh stored procedures.

Note: The default values apply to all databases, unless otherwise specified on the **Databases** tab.

Databases Tab

The **Databases** tab on the **Create Multiple DB Aliases** dialog allows you to provide explicit information for each DB Alias.

Sel

Select the check box to create a DB Alias for the database. If you do not want to create a DB Alias, clear the check box. This grid column is locked in position, so you can scroll to the left or right and still see the selections for the databases.

Note: If a DB Alias for a database exists, the grid row is protected and shaded.

Database Name

The name assigned to the database when it was created.

DB Alias Name

The identifier that allows the software to access the database. This name also serves as the high-level qualifier for database table names. This entry is required, and is populated with the database name in uppercase, by default.

DB Alias Description

Text that describes or explains the purpose of the DB Alias.

Procedure Action

Options to create/refresh procedures or use existing procedures. To select an option, click the grid cell and click the down arrow.

Note: When creating procedures to be shared for access to all Sybase ASE or SQL Server databases on the server, this grid cell is protected. The first selected entry is displayed as Create/ Refresh; other selected entries to use the shared stored procedures display Use Existing.

Procedure Qualifier

The high-level qualifier for stored procedures. If blank, the entry on the **Stored Procedure Defaults** tab is used. For Sybase ASE databases sharing stored procedures, the entry "sp_" is displayed and cannot be edited.

Grant Auth ID

An identifier for users authorized to maintain stored procedures. Specify a User ID, Group Name, or **Public**. If blank, the entry on the **Stored Procedure Defaults** tab is used.

Logon User ID

User ID (up to 30 characters) required to create/refresh stored procedures. If blank, the entry on the **Logon Defaults** tab is used.

Logon Password

The password (up to 30 characters) required to create/refresh stored procedures. If blank, the entry on the **Logon Defaults** tab is used.

Saved User ID

The User ID (up to 30 characters) required to logon using the DB Alias. This identifier is saved to the Windows registry of the workstation. If blank, the entry on the **Saved Logon Defaults** tab is used.

Saved Password

The password (up to 30 characters) required to logon using the DB Alias. If blank, the entry on the **Saved Logon Defaults** tab is used.

Note: You can change the **Saved User ID** and **Saved Password** when you configure options and when you set Personal Options.

Always Ask for Password

Select this check box to require a password each time you connect to the database. If you clear this check box, you need not supply a password on future attempts to connect to the database.

Create Primary Keys

Select this check box to create primary keys, as needed, for the database.

To create primary keys from within the **Configuration** program, select **Create Primary Keys** from the **Tasks** menu on the main window.

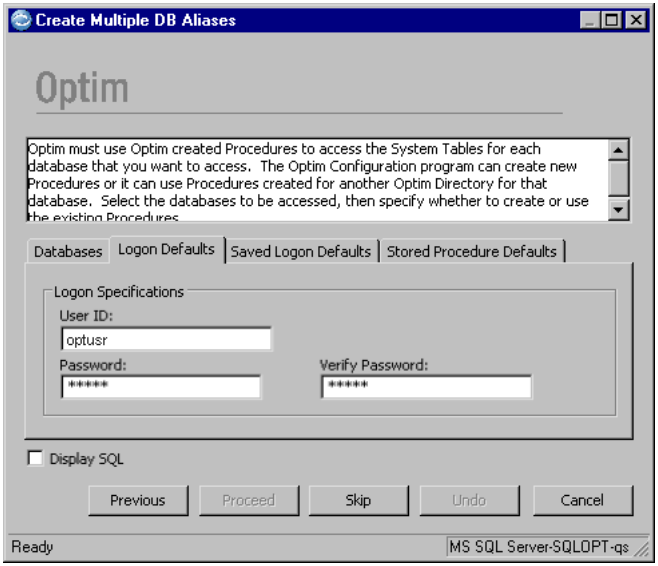
To create primary keys from within ***Optim***, select **New** from the **File** menu and select **Primary Keys** from the **Definitions** submenu on the main window.

Display SQL

Select this check box to display SQL statements before creating or dropping stored procedures.

Logon Defaults Tab

Use the **Logon Defaults** tab to provide the default **User ID** and **Password** required to create/refresh stored procedures.

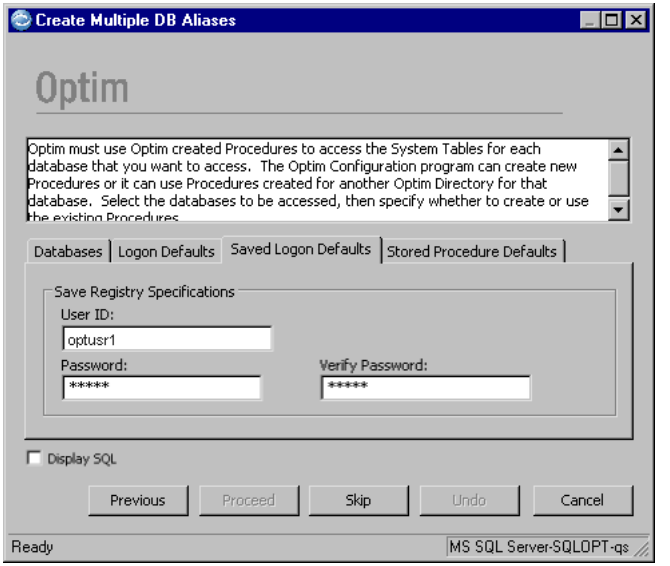

Create Multiple DB Aliases
Optim
Optim must use Optim created Procedures to access the System Tables for each database that you want to access. The Optim Configuration program can create new Procedures or it can use Procedures created for another Optim Directory for that database. Select the databases to be accessed, then specify whether to create or use the existing Procedures
Databases
Logon Defaults
Saved Logon Defaults
Stored Procedure Defaults
Logon Specifications
User ID:
optusr
Password:
Verify Password:
Display SQL
Previous
Proceed
Skip
Undo
Cancel
Ready
MS SQL Server-SQLOPT-qs

The entries on the **Logon Defaults** tab allow you to connect to the database while configuring a workstation. You must enter the password a second time for verification.

Note: The default logon information applies to all DB Aliases unless you provide explicit logon information on the **Databases** tab.

Saved Logon Defaults

Use the **Saved Logon Defaults** tab to provide the **User ID** and **Password** needed to access the DB Alias.


Create Multiple DB Aliases
Optim
Optim must use Optim created Procedures to access the System Tables for each database that you want to access. The Optim Configuration program can create new Procedures or it can use Procedures created for another Optim Directory for that database. Select the databases to be accessed, then specify whether to create or use the existing Procedures
Databases
Logon Defaults
Saved Logon Defaults
Stored Procedure Defaults
Save Registry Specifications
User ID:
optusr1
Password:
*****
Verify Password:
*****
Display SQL
Previous
Proceed
Skip
Undo
Cancel
Ready
MS SQL Server-SQLOPT-qs

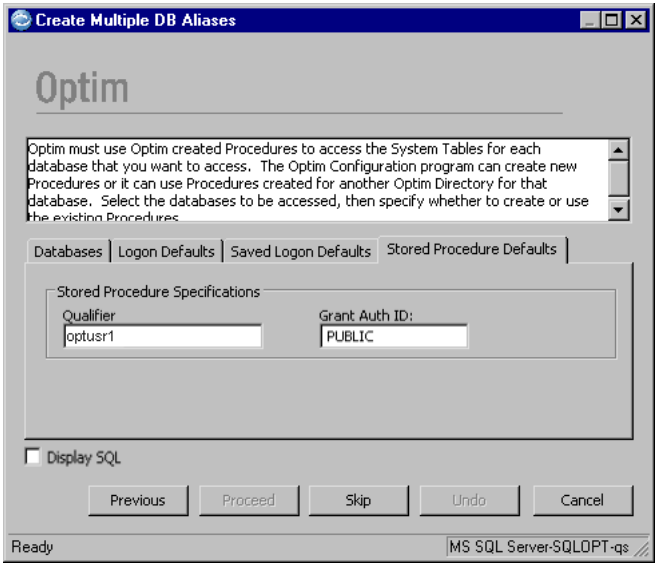
The entries on the **Saved Logon Defaults** tab allow you to save registry entries to access the databases. You must enter your password a second time for verification.

- To modify the saved **User ID** and **Password** from within the **Configuration** program, select **Configure Options** from the main window and edit Personal Options.
- To modify the **User ID** and **Password** from within ***Optim***, select **Personal** from the **Options** menu on the main window and edit the **Logon** tab.

Note: The default saved logon information applies to all DB Aliases unless you provide explicit logon information on the **Databases** tab.

Stored Procedure Defaults

Use the **Stored Procedure Defaults** tab to provide the procedure **Qualifier** and **Grant Auth ID** required to create/refresh stored procedures.


Create Multiple DB Aliases
Optim
Optim must use Optim created Procedures to access the System Tables for each database that you want to access. The Optim Configuration program can create new Procedures or it can use Procedures created for another Optim Directory for that database. Select the databases to be accessed, then specify whether to create or use the existing Procedures
Databases
Logon Defaults
Saved Logon Defaults
Stored Procedure Defaults
Stored Procedure Specifications
Qualifier
optusr1
Grant Auth ID:
PUBLIC
Display SQL
Previous
Proceed
Skip
Undo
Cancel
Ready
MS SQL Server-SQLOPT-qs

Note: The default stored procedure information applies to all DB Aliases unless you provide explicit stored procedure information on the **Databases** tab.

When you enter the necessary information on each tab and click **Proceed**, the **Configuration** program connects to the database, catalogs the stored procedures, writes the registry entries, and optionally creates primary keys. These four steps are repeated automatically for each selected database. When complete, the next step is to configure security.

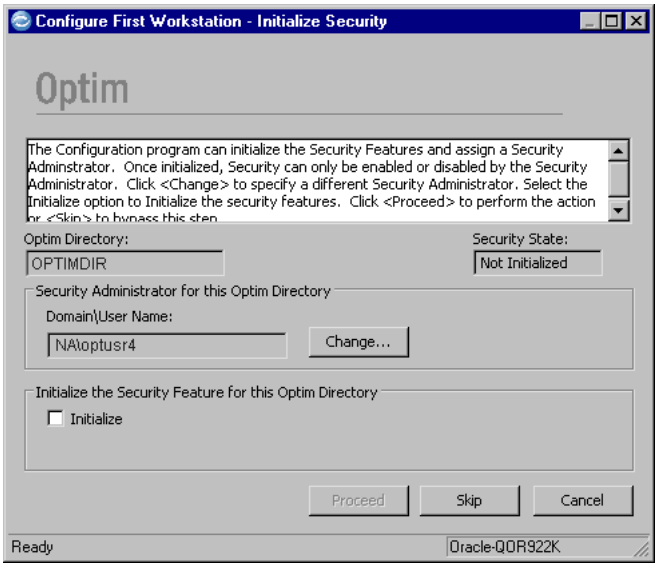
5.1.4 Optim Security

Optim Security includes three features: Archive File Security, Functional Security, and Object Security. For more information about these security features, see **Appendix D. Optim Security**.

To use ***Optim*** Security, security must be initialized for the Directory.

Initialize Security/Change Security Administrator

Use the **Initialize Security** dialog to assign a Security Administrator for the ***Optim*** Directory and initialize security. If security has been initialized for the Directory, this dialog is replaced by the **Change Security Administrator** dialog, which is similar to **Initialize Security**, but with no initialize option.


Configure First Workstation - Initialize Security
Optim
The Configuration program can initialize the Security Features and assign a Security Adminstrator. Once initialized, Security can only be enabled or disabled by the Security Administrator. Click <Change> to specify a different Security Administrator. Select the Initialize option to Initialize the security features. Click <Proceed> to perform the action
Optim Directory:
OPTIMDIR
Security State:
Not Initialized
Security Administrator for this Optim Directory
Domain\User Name:
NA\optusr4
Change...
Initialize the Security Feature for this Optim Directory
Initialize
Proceed
Skip
Cancel
Ready
Oracle-QOR922K

Optim Directory displays the Directory name, and **Security State** indicates that security is *Not Initialized*.

Security Administrator for this Optim Directory

The Security Administrator is assigned to the ***Optim*** Directory when security is initialized. Only one Security Administrator can be assigned to an ***Optim*** Directory. The Security Administrator can configure ***Optim*** Security as well as control access to the default Access Control Domain (ACD) and Access Control List (ACL) for the Directory. For more information, see **Appendix D. Optim Security**.

Use **Security Administrator for this Optim Directory** to identify the Security Administrator by the two-part **Domain\User Name**. By default, the Security Administrator is the user signed on to the workstation. To specify another user, click **Change** to open the **Specify Domain Connection Information** dialog, which allows you to enter a different Domain\User Name or select from a list of user accounts in an available domain. The Security Administrator must be a user account in a network domain that is accessible from the current workstation.

Note: You can also change the Security Administrator using the **Change Security Administrator** dialog, available by selecting **Configure Security for an Optim Directory** from the **Tasks** menu.

Initialize the Security Feature for this Optim Directory

After identifying the Security Administrator, initialize security for the Directory by selecting **Initialize** and clicking **Proceed**. When security is initialized, the Security Administrator is assigned, and a default ACD and ACL are created for the Directory. For more information about ACDs and ACLs, see **Appendix D. Optim Security**.

Once security has been initialized for an ***Optim*** Directory, it cannot be undone; however, the Security Administrator can enable or disable the ***Optim*** Security features for the Directory by selecting the **Configure Security for an Optim Directory** option from the **Tasks** menu in the Configuration main window.

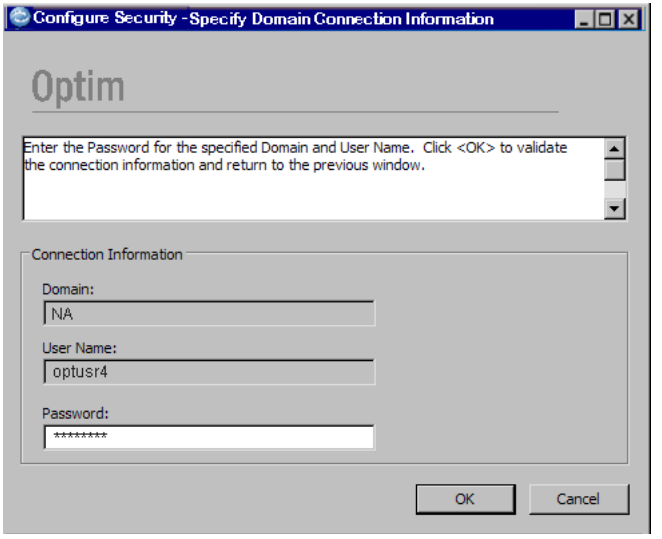
If you do not wish to establish security for the Directory, click **Skip**. To initialize security at a later time, use the **Configure Security for an Optim Directory** option. For more information about enabling, disabling, and configuring the ***Optim*** Security features, see **7.4 Configure Security for an Optim Directory** on page 192.

Click **Skip** or **Cancel** to exit the security configuration process. Security will not be initialized and the Security Administrator will not be changed.

Specify Domain Connection Information

Use the **Specify Domain Connection Information** dialog to identify the Security Administrator. Enter the **Domain**, **User Name**, and **Password** for the Security Administrator, or click **Browse** to select a user from the **Security Users** dialog. If you select a user, you must

enter the user password when you return to the **Specify Domain Connection Information** dialog.

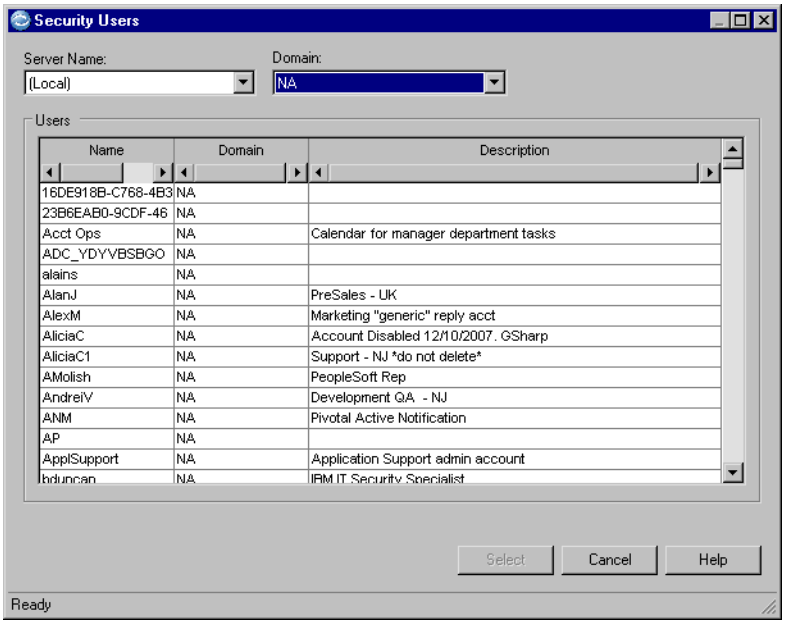


Click **OK** to return to the **Initialize Security** dialog.

Security Users

The **Security Users** dialog allows you to select a user from an available domain. Select a **Server Name** and a **Domain** to list **Users** in the domain. After selecting a user, click **Select** to return to the **Specify**

Domain Connection Information dialog, which will display the selected **Domain** and **User Name**.



Notes:

- If your site does not use a ***Server***, (Local) is displayed in **Server Name**.
- If a UNIX or Linux **Server Name** is selected, the node name is displayed in **Domain**.

5.1.5 Configure Options

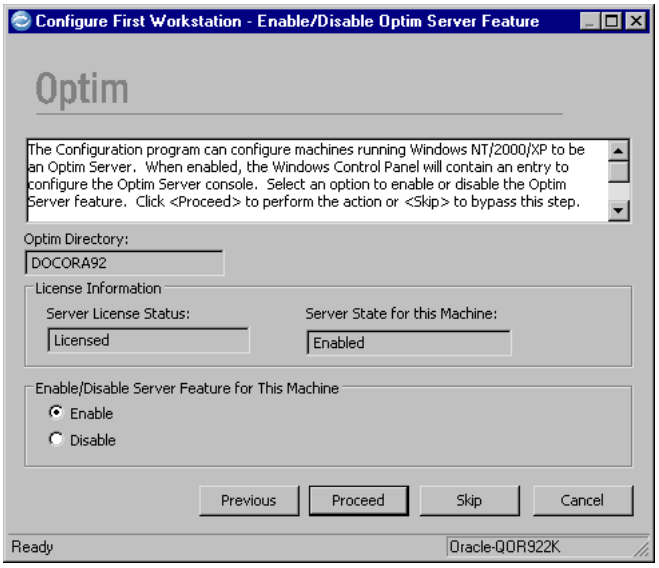
In the following steps, you can:

- Designate a machine as a ***Server*** (if this feature is licensed).
- Enable the ODBC interface for the machine (if ***Archive*** is licensed).
- Specify a Product Configuration File to record Product Options that, in most cases, apply to all ***Optim*** users at a site.
- Configure Personal Options that are stored in the Windows registry on a particular workstation.

Note: Both the Product Configuration File and the registry entries are created during the configuration process.

Enable/Disable Optim Server Feature

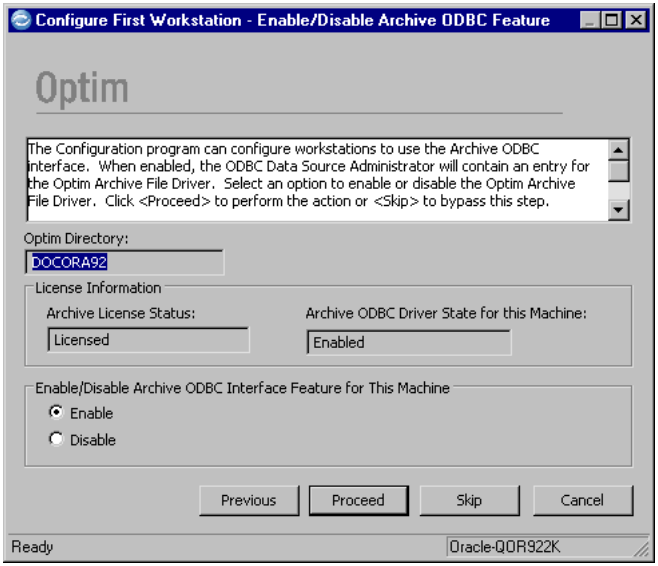
On the **Enable/Disable Optim Server Feature** dialog, choose to enable or disable the current machine as a ***Server***.


Configure First Workstation - Enable/Disable Optim Server Feature
Optim
The Configuration program can configure machines running Windows NT/2000/XP to be an Optim Server. When enabled, the Windows Control Panel will contain an entry to configure the Optim Server console. Select an option to enable or disable the Optim Server feature. Click <Proceed> to perform the action or <Skip> to bypass this step.
Optim Directory:
DOCORA92
License Information
Server License Status:
Licensed
Server State for this Machine:
Enabled
Enable/Disable Server Feature for This Machine
Enable
Disable
Previous
Proceed
Skip
Cancel
Ready
Oracle-QOR922K

If the site is not licensed for the ***Server***, **Enable** is not available. Refer to **Chapter 6. Configure the Optim Server** for information needed to configure the ***Server***.

Enable/Disable Archive ODBC Feature

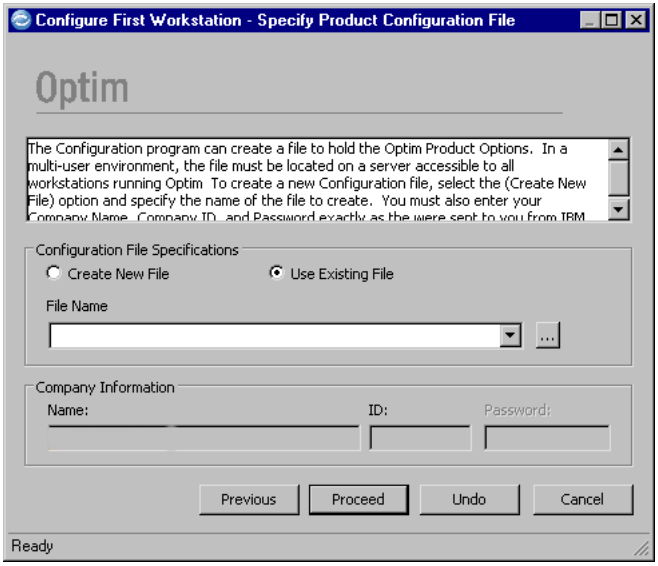
On the **Enable/Disable Archive ODBC Feature** dialog, choose to enable or disable the ODBC driver for the current machine.


Configure First Workstation - Enable/Disable Archive ODBC Feature
Optim
The Configuration program can configure workstations to use the Archive ODBC interface. When enabled, the ODBC Data Source Administrator will contain an entry for the Optim Archive File Driver. Select an option to enable or disable the Optim Archive File Driver. Click <Proceed> to perform the action or <Skip> to bypass this step.
Optim Directory:
DOCORA92
License Information
Archive License Status:
Licensed
Archive ODBC Driver State for this Machine:
Enabled
Enable/Disable Archive ODBC Interface Feature for This Machine
Enable
Disable
Previous
Proceed
Skip
Cancel
Ready
Oracle-QOR922K

If your site is not licensed for ***Archive***, **Enable** is not available.

Specify Product Configuration File

Use the **Specify Product Configuration File** dialog to provide the complete directory path and name of the configuration file.


Configure First Workstation - Specify Product Configuration File
Optim
The Configuration program can create a file to hold the Optim Product Options. In a multi-user environment, the file must be located on a server accessible to all workstations running Optim To create a new Configuration file, select the (Create New File) option and specify the name of the file to create. You must also enter your
Configuration File Specifications
Create New File
Use Existing File
File Name
Company Information
Name:
ID:
Password:
Previous
Proceed
Undo
Cancel
Ready

The **Specify Product Configuration File** dialog includes the following:

Configuration File Specifications

Create New File — Select this option to create a new Product Configuration File.

Use Existing File — Select this option to use an existing Product Configuration File.

File Name — Provide the complete directory path and name of the Product Configuration File. To select a file from your system directories, click the browse button.

Note: The Configuration File is usually shared by all users at a site; specify a path on a file server that is easily accessible to all users.

Company Information

Name — Name of the company licensed to use ***Optim***.

ID — Company identifier required for using ***Optim***.

Password — Enter the password required for creating a new Product Configuration File.

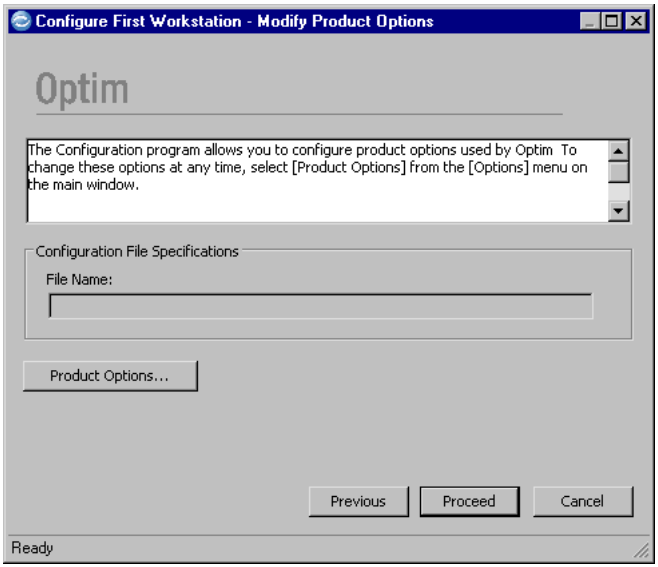
Note: The password is provided by email when the product is shipped.

Modify Product Options

Optim is distributed with standard settings for Product Options. The **Modify Product Options** dialog allows you to customize these settings to accommodate conditions at your site.

If the ***Optim*** Directory is in multi-byte format, you will be prompted to use Product Options to indicate how ***Optim*** should handle round trip

errors. For more information, see **MBCS Roundtrip Processing** on page 255.


Configure First Workstation - Modify Product Options
Optim
The Configuration program allows you to configure product options used by Optim To change these options at any time, select [Product Options] from the [Options] menu on the main window.
Configuration File Specifications
File Name:
Product Options...
Previous
Proceed
Cancel
Ready

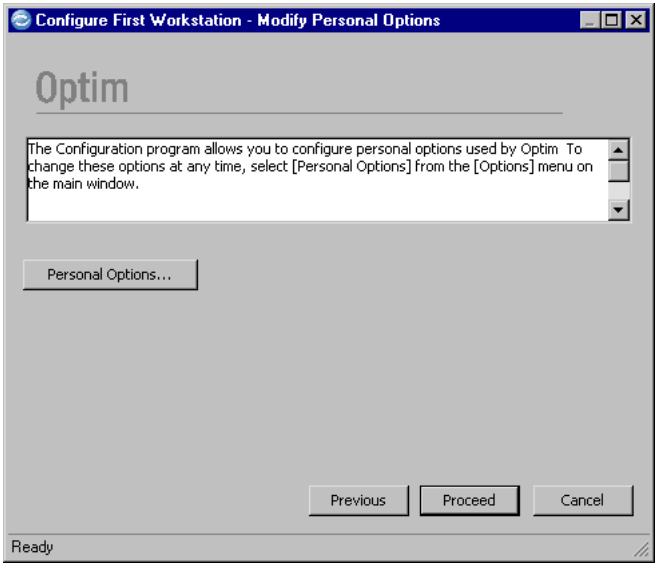
The name of the Product Configuration File specified in the preceding dialog is displayed. If you click **Product Options**, you are prompted for a password to open the **Product Options** dialog.

Note: You must have a password to review and change Product Options. ***Optim*** is distributed with the case-sensitive password *optim*. You can change this password when configuring the first workstation.

For a detailed description of the **Product Options** dialog, refer to **8.2 Using the Editor** on page 248. After you modify Product Options and return to the **Modify Product Options** dialog, click **Proceed** to open the next dialog in the process.

Modify Personal Options

The **Modify Personal Options** dialog is similar to the **Modify Product Options** dialog.

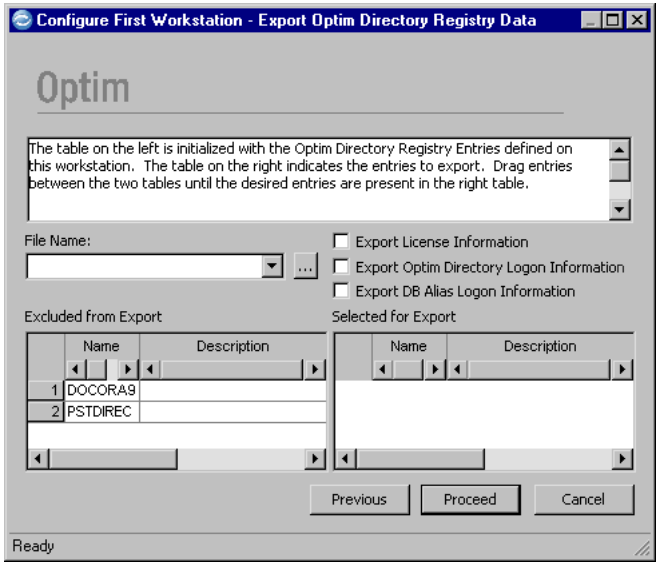

Configure First Workstation - Modify Personal Options
Optim
The Configuration program allows you to configure personal options used by Optim To change these options at any time, select [Personal Options] from the [Options] menu on the main window.
Personal Options...
Previous
Proceed
Cancel
Ready

Click **Personal Options** to open the **Personal Options** dialog. A detailed description of this dialog is provided in **9.2 Using the Editor** on page 282. After you modify Personal Options and return to the **Modify Personal Options** dialog, click **Proceed** to open the next dialog in the process.

5.1.6 Export Registry Data

If you intend to configure several workstations, you can save time by exporting the ***Optim*** Directory registry data to a file and saving the file to a directory that is easily accessible. During the process of configuring the first workstation, you are prompted to export registry data, or you can select **Export Registry Data** from the **File** menu on the Configuration main window.

The **Export Optim Directory Registry Data** dialog allows you to specify an output file name and select the registry entries and other information you want to export.


Configure First Workstation - Export Optim Directory Registry Data
Optim
The table on the left is initialized with the Optim Directory Registry Entries defined on this workstation. The table on the right indicates the entries to export. Drag entries between the two tables until the desired entries are present in the right table.
File Name:
Export License Information
Export Optim Directory Logon Information
Export DB Alias Logon Information
Excluded from Export
Selected for Export
Name
Description
1 DOCORA9
2 PSTDIREC
Previous
Proceed
Cancel
Ready

The **Export Optim Directory Registry Data** dialog includes the following:

File Name

Enter the name of the file to which you want to export the registry data. The file name uses a default **.txt** extension. To select from your system directories, click the browse button.

Note: If you do not provide the full directory path and file name, the file is saved to the Data Directory identified in Personal Options.

Export . . .

Select one or all check boxes to export:

- Product License information
- Optim Directory Logon information
- DB Alias Logon information

Excluded from Export

List of ***Optim*** Directories not selected for exporting registry data.

Name	Name of each available ***Optim*** Directory.
Description	Text that describes or explains the purpose of the ***Optim*** Directory.

Selected for Export

List of ***Optim*** Directories selected for export.

Name	Name of each selected ***Optim*** Directory.
Description	Text that describes or explains the purpose of the ***Optim*** Directory.

Move an item from one list to the other by dragging the name. Also, to rearrange listed items, drag the line number to the new position.

After you make your selections, click **OK** to export the registry data.

Complete

When you finish, the configuration process opens the **Complete** dialog. This dialog describes the files that may be created during the process.

SQL.TXT	Contains the DDL statements generated to carry out various functions.
BIND.TXT	Contains the DB2 Bind Report.
KEYS.TXT	Contains a list of the ***Optim*** Keys created.
PR0CNFG.LOG	Contains the Configuration Processing Log.

These files are located in the Temporary Work Directory, specified using the **General** tab of the **Personal Options** dialog. You can browse or print these files using a text editor, such as *Notepad*.

On the **Complete** dialog, click **Close** to return to the Configuration main window, where you can quit the program or prepare to configure the next workstation.

5.1.7 Summary

The tasks for configuring the first workstation are complete, including the following:

- Create an ***Optim*** Directory and corresponding Windows registry entries.
- Create a DB Alias for each database within the ***Optim*** Directory.
- Create ***Optim*** Primary Keys for database tables that did not have DBMS primary keys but did have a unique index.
- Load sample database tables.
- Create and load the data privacy data tables, if you have an ***Optim*** Data Privacy License.
- Initialize ***Optim*** Security and assign the Security Administrator.
- Create the Product Configuration File and modify Product and Personal Options.
- Export registry data to ease the task of configuring additional workstations.

5.2 Configure Additional Workstation

After you configure the first workstation, you can configure any additional workstations to use ***Optim***. This task uses ***Optim*** Directory and DB Aliases created while configuring the first workstation. However, you must create a Windows registry entry on each additional workstation to permit access to the ***Optim*** Directory. You may also configure Personal Options for each workstation.

Note: If the configuration at your site requires, you may create a separate Product Configuration File for an individual workstation; however, the typical installation uses one Configuration File that is easily accessible to all users.

Guidelines

When you configure additional workstations, the following guidelines apply.

- Even if you install ***Optim*** on a server that allows access to each workstation, you must run **Setup** before configuring each additional workstation. This step ensures that the Windows registry for the workstation is properly prepared and desktop icons are created.
- If you run **Setup** for a workstation with the ***Optim*** software on a file server, you must identify the server directory in which ***Optim*** is installed as the **Destination Folder**.

You can start the process of configuring additional workstations in the following ways:

- Start the **Configuration Assistant** immediately after **Setup** completes. Clear the **Configure the First Workstation** check box and click **Proceed**. On the next dialog, select the **Configure Additional Workstation** check box.
- Select **Configuration Assistant** from the **Help** menu on the Configuration main window. Clear the **Configure the First Workstation** check box and click **Proceed**. On the next dialog, select the **Configure Additional Workstation** check box.
- Select **Configure Additional Workstation** from the **Tasks** menu on the Configuration main window.

If you exported registry data after configuring the first workstation, you can save time by importing it to additional workstations. You are prompted to import ***Optim*** Directory registry data when configuring each additional workstation. If you choose not to import registry data,

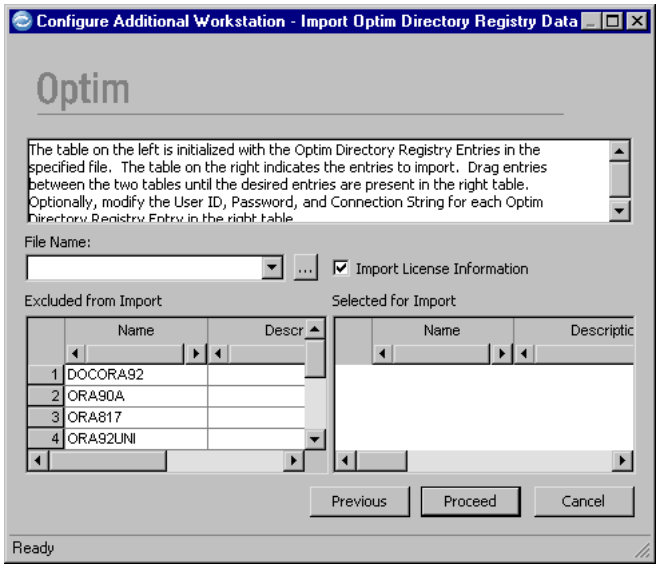
you must first enter the Product License Key and select the option to **Create a new Registry Entry for Existing Optim Directory**.

5.2.1 Import Registry Entries

If you intend to configure several workstations, you can save time by importing ***Optim*** Directory registry data and the Product License Key from a file.

Note: Before you can import registry data, you must export the data to a file. You can export the data during the process of configuring the first workstation or you can select **Export Registry Data** from the **File** menu on the Configuration main window.

You can import registry data during the process of configuring an additional workstation or you can select **Import Registry Data** from the **File** menu. The **Import Optim Directory Registry Data** dialog allows you to import registry entries and license information.


Configure Additional Workstation - Import Optim Directory Registry Data
Optim
The table on the left is initialized with the Optim Directory Registry Entries in the specified file. The table on the right indicates the entries to import. Drag entries between the two tables until the desired entries are present in the right table. Optionally, modify the User ID, Password, and Connection String for each Optim
File Name:
Import License Information
Excluded from Import
Selected for Import
Name
Descr
Name
Descriptic
1 DOCORA92
2 ORA90A
3 ORA817
4 ORA92UNI
Previous
Proceed
Cancel
Ready

The **Import Optim Directory Registry Data** dialog includes the following:

File Name

Enter the name of the file that contains the ***Optim*** Directory registry data you want to import.

Import License Information

Select this check box to import license information, if available in the specified file.

Excluded from Import

List of available ***Optim*** Directories not selected for importing registry data. Move an item from one list to the other by dragging the name. Also, to rearrange listed items, drag the line number to the new position.

Name Name of each available ***Optim*** Directory.

Description Text that describes or explains the purpose of the ***Optim*** Directory.

Selected for Import

List of ***Optim*** Directories selected for import. Move an item from one list to the other by dragging the name. Also, to rearrange listed items, drag the line number to the new position.

Name Name of each selected ***Optim*** Directory.

Description Text that describes or explains the purpose of the ***Optim*** Directory.

User ID Identifier (up to 30 characters) that the DBMS requires to permit access to the ***Optim*** Directory. You can modify this entry.

Password Password (1 to 30 characters) that corresponds to the specified User ID. You can modify this entry.

- The database administrator usually defines User IDs and passwords.
- This password is used only by the DBMS. Sybase ASE and SQL Server passwords are case sensitive.

Connection String

String (or name) that permits a workstation to access the database. The DBMS uses this connection string to recognize the database. You can modify this entry.

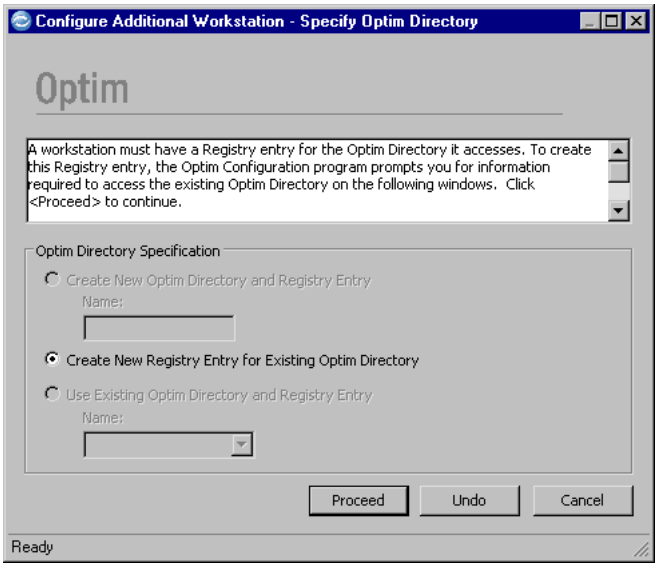
- For some database management systems, it is possible to define a different Connection String for each workstation to access the same database.
- For Sybase ASE and SQL Server, the Connection String refers to the network name of the computer where the database resides.

5.2.2 Create Registry Entry

If you elect not to import ***Optim*** Directory registry data, you must create a new registry entry for each workstation to use the ***Optim*** Directory. You must identify the ***Optim*** Directory and the associated DBMS, and provide information to connect to the database.

Specify Optim Directory

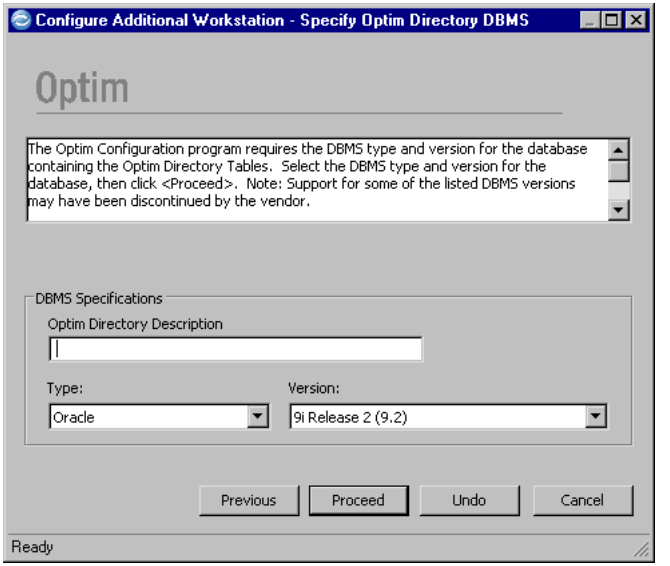
The opening dialog for configuring an additional workstation is the **Specify Optim Directory** dialog. Use this dialog to create a Windows registry entry.


Configure Additional Workstation - Specify Optim Directory
Optim
A workstation must have a Registry entry for the Optim Directory it accesses. To create this Registry entry, the Optim Configuration program prompts you for information required to access the existing Optim Directory on the following windows. Click <Proceed> to continue.
Optim Directory Specification
Create New Optim Directory and Registry Entry
Name:
Create New Registry Entry for Existing Optim Directory
Use Existing Optim Directory and Registry Entry
Name:
Proceed
Undo
Cancel
Ready

The only option available when configuring an additional workstation is selected when the dialog opens. To **Create New Registry Entry for Existing Optim Directory**, click **Proceed**.

Specify Optim Directory DBMS

The next step in creating the Windows registry entry is to **Specify Optim Directory DBMS**.


Configure Additional Workstation - Specify Optim Directory DBMS
Optim
The Optim Configuration program requires the DBMS type and version for the database containing the Optim Directory Tables. Select the DBMS type and version for the database, then click <Proceed>. Note: Support for some of the listed DBMS versions may have been discontinued by the vendor.
DBMS Specifications
Optim Directory Description
Type:
Oracle
Version:
9i Release 2 (9.2)
Previous
Proceed
Undo
Cancel
Ready

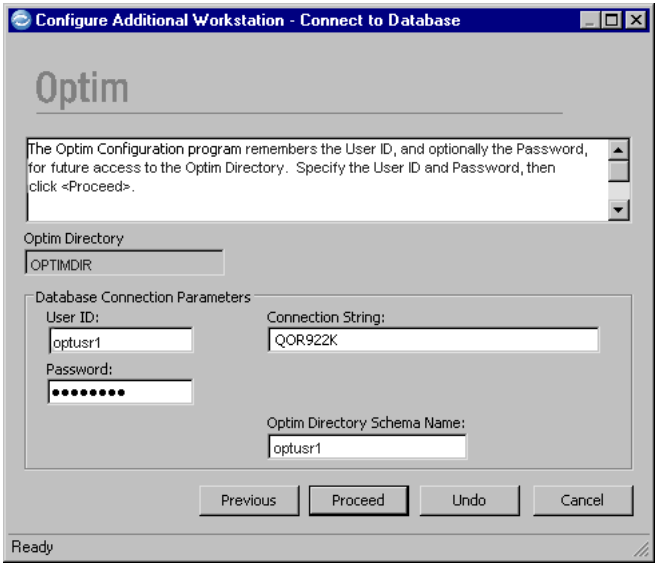
The **Specify Optim Directory DBMS** dialog includes the following details. (When the dialog opens, **Optim Directory Description**, **Type**, and **Version** is populated with any previously entered information.)

DBMS Specifications

Optim Directory Description	Provide text that describes or explains the purpose of the ***Optim*** Directory (up to 40 characters). This is useful if you have multiple Optim Directories.
Type	Select the type of DBMS software. To select from a list, click the down arrow. The selected DBMS appears on the status bar of subsequent dialogs in the process.
Version	Select the version of the DBMS software. To select from a list, click the down arrow.

Connect to Database

The **Connect to Database** dialog allows you to provide database connection information for the ***Optim*** Directory registry entry.



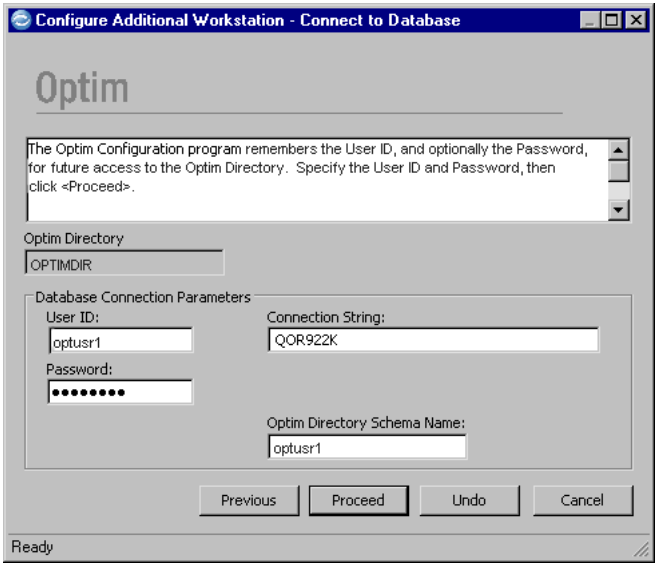
When configuring the workstation, you must provide a **User ID**, **Password**, and **Connection String** that allows the workstation to connect to the database and access ***Optim*** Directory tables. If you are using Sybase ASE, SQL Server, or Informix, you must indicate the **DB Name**. Also, provide the identifier (**Creator ID**, **Schema Name**, or **Owner ID**) for ***Optim*** Directory tables.

Note: For some database management systems, the identifier for ***Optim*** Directory tables must match the identifier used to create the ***Optim*** Directory, including case.

The configuration process locates the ***Optim*** Directory and displays a confirmation message. Click **No** to cancel the function and return to the main window or click **Yes** to create a registry entry for the ***Optim*** Directory and display a second **Connect to Database** dialog.

Connect to Database – Subsequent Access

On the next dialog, you are prompted to provide the **User ID** and **Password** for subsequent access to the ***Optim*** Directory from the workstation.

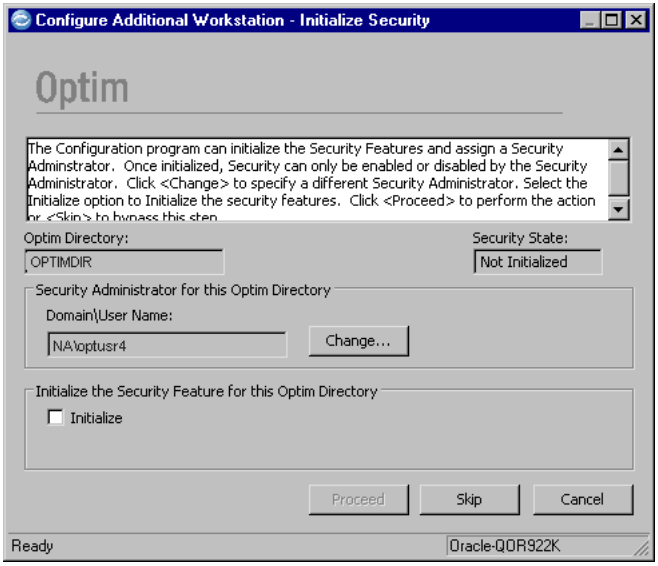


Subsequent steps allow you to initialize ***Optim*** Security or assign a Security Administrator, designate the workstation as a ***Server*** (if the optional ***Server*** feature is licensed), enable the ODBC Interface feature (if ***Archive*** is licensed), specify a Product Configuration File, and configure Product and Personal Options. Click **Proceed** to continue.

5.2.3 Initialize Security/Change Security Administrator

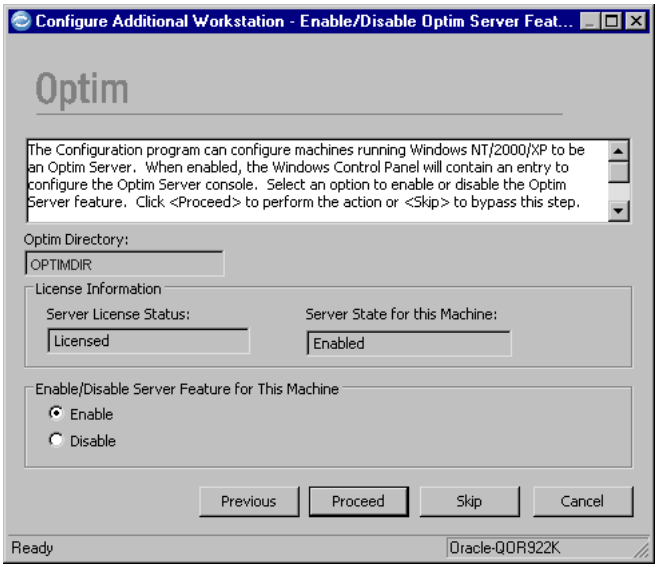
On the **Initialize Security** dialog, assign a Security Administrator for the PST Directory and initialize security. If security has been initialized for the Directory, this dialog is replaced by the **Change Security Administrator** dialog, which is similar to **Initialize Security**, but with no initialize option.

For information about initializing ***Optim*** Security and assigning a Security Administrator, see **5.1.4 Optim Security**.


Configure Additional Workstation - Initialize Security
Optim
The Configuration program can initialize the Security Features and assign a Security Adminstrator. Once initialized, Security can only be enabled or disabled by the Security Administrator. Click <Change> to specify a different Security Administrator. Select the Initialize option to Initialize the security features. Click <Proceed> to perform the action
Optim Directory:
OPTIMDIR
Security State:
Not Initialized
Security Administrator for this Optim Directory
Domain\User Name:
NA\optusr4
Change...
Initialize the Security Feature for this Optim Directory
Initialize
Proceed
Skip
Cancel
Ready
Oracle-QOR922K

5.2.4 Enable/Disable Optim Server Feature

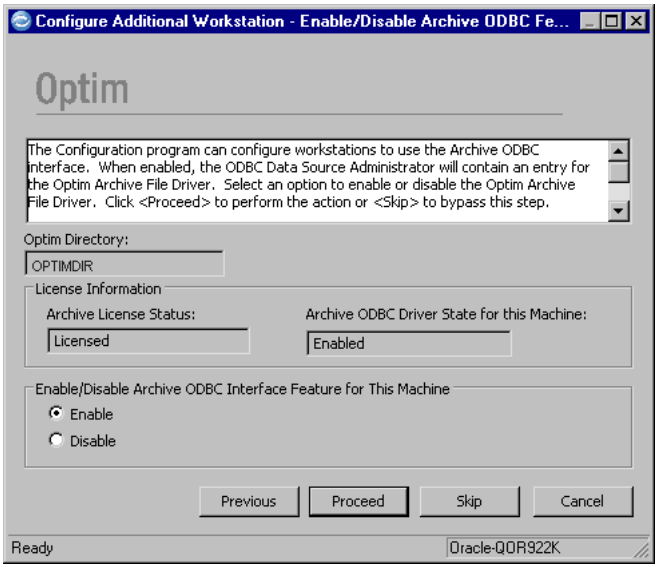
On the **Enable/Disable Optim Server Feature** dialog, indicate whether to enable or disable the current machine as a ***Server***.


Configure Additional Workstation - Enable/Disable Optim Server Feat...
Optim
The Configuration program can configure machines running Windows NT/2000/XP to be an Optim Server. When enabled, the Windows Control Panel will contain an entry to configure the Optim Server console. Select an option to enable or disable the Optim Server feature. Click <Proceed> to perform the action or <Skip> to bypass this step.
Optim Directory:
OPTIMDIR
License Information
Server License Status:
Licensed
Server State for this Machine:
Enabled
Enable/Disable Server Feature for This Machine
Enable
Disable
Previous
Proceed
Skip
Cancel
Ready
Oracle-QOR922K

If the ***Server*** is not licensed, **Enable** is not available. Refer to **Chapter 6. Configure the Optim Server** for information needed to configure the ***Server***.

5.2.5 Enable/Disable Archive ODBC Interface

On the **Enable/Disable Archive ODBC Interface** dialog, indicate whether to enable or disable the ODBC driver for the current machine.


Configure Additional Workstation - Enable/Disable Archive ODBC Fe...
Optim
The Configuration program can configure workstations to use the Archive ODBC interface. When enabled, the ODBC Data Source Administrator will contain an entry for the Optim Archive File Driver. Select an option to enable or disable the Optim Archive File Driver. Click <Proceed> to perform the action or <Skip> to bypass this step.
Optim Directory:
OPTIMDIR
License Information
Archive License Status:
Licensed
Archive ODBC Driver State for this Machine:
Enabled
Enable/Disable Archive ODBC Interface Feature for This Machine
Enable
Disable
Previous
Proceed
Skip
Cancel
Ready
Oracle-QOR922K

If the site is not licensed for ***Archive***, **Enable** is not available.

5.2.6 Specify Product Configuration File

After you create the Windows registry entry for the ***Optim*** Directory, you must identify the Product Configuration File for the workstation. The configuration process opens the **Specify Product Configuration File** dialog.

Note: If you decide to install ***Optim*** on a server or on each workstation, all workstations can use one Product Configuration File, located on the server.

You create the Product Configuration File when you configure Product Options for the first workstation. Therefore, when you configure an additional workstation, select **Use Existing File** and specify the fully qualified name of the original Product Configuration File on the **Specify Product Configuration File** dialog. For more complete information, refer to **5.1.5 Configure Options**.

5.2.7 Summary

The tasks for Configuring an Additional Workstation are complete.

- Import registry data, or create a Windows registry entry for the workstation to access the ***Optim*** Directory.
- Identify a Product Configuration File for the workstation.

You must repeat these steps for each workstation you want to use with ***Optim***.

After you configure the first workstation and any additional workstations, you are ready to configure the ***Server*** component, if licensed for it, and carry out the other tasks available from the **Tasks** menu. The following chapters describe how to configure the ***Server*** and perform other tasks.

6. Configure the *Optim Server*

The ***Server*** option allows users to define tasks on a workstation and direct resource-intensive data processing functions to a machine more suited to the task. When a task requires the movement, processing or storage of very large volumes of data, the request can be defined at the workstation in the normal way, then directed for remote processing on the machine hosting the ***Server***. If this machine is the machine on which the database is running, network traffic associated with the movement of data is eliminated. You can also install the ***Server*** on a machine dedicated to the ***Server*** function. In addition, a ***Server*** is required to process from a database residing in a UNIX environment and to support access to archived data using IBM's Open Data Manager.

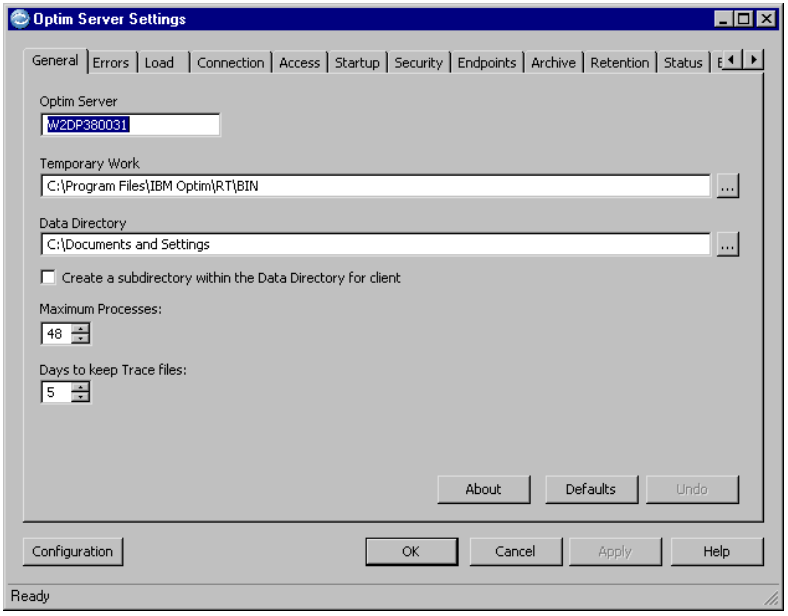
Note: In a UNIX environment, the ***Server*** is installed from a console and configured using the Command Line Interface. (See **Appendix A. Install and Configure the Server under UNIX or Linux** for complete information.)

To configure the ***Server*** option on a Windows workstation, you must first install ***Optim***, and run the **Configuration** program to configure the workstation and enable it as a ***Server***. (Refer to **7.5 Enable/Disable this Machine as an Optim Server** on page 201.)

After you activate the workstation as a ***Server***, you must configure it using the **Optim Server Settings** Control Panel applet.

Control Panel

Double-click the ***Optim*** icon in the Windows Control Panel to run the **Optim Server Settings** applet, which allows you to provide settings unique to the server, such as the path and executable file name for each database loader, connection strings for all DB Aliases, and protocols for access to the server.



Tabs

The tabs on the **Optim Server Settings** dialog are described in the following paragraphs. Detailed information is provided in the following sections.

General The default Temporary Work Directory and Data Directory.

Errors Font characteristics for displays of informational, warning, and error messages. Indicate the maximum number of lines displayed in the message bar and whether to hide the message bar when empty.

Load The path and name of the executable required to gain access to each DBMS Loader.

Connection Connect strings for all DB Aliases in an ***Optim*** Directory.

Access Access to specific ***Server*** drives and directories.

Startup	Type of start up for the ***Server***.
Security	The source of User ID and password information to log on.
Endpoints	Protocol and address information for machines hosting the ***Server***.
Archive	Directories for storing Archive files and Archive Index files.
Retention	Options to scan ***Optim*** Directories for Archive Files with a retention policy.
Status	Current workstation connections to machines hosting the ***Server***.
Email	Email addresses for report messages.

As part of the installation process, you create entries in the Current User registry.

Note: When you add or delete an ***Optim*** Directory or DB Alias using the **Configuration** program, you should also apply the new settings to the ***Server***.

Configuration

You can keep Local Machine registry entries for the ***Server*** separate from those for the user by entering information in the **Optim Server Settings** dialog. Settings on the **Optim Configuration** dialog pertain only to the ***Server*** component, not to the currently logged on user.

Note: If workstations are processing, setting changes are saved when you click **Apply**, but are not applied until all processing completes. The ***Server*** rejects new connections until the current connections terminate and the new settings are applied. Scheduled processes are similarly rejected when settings are pending. Scheduled processes are retried until the Stop Time entered in the Scheduling Editor.

Credentials

For information about user credentials required to run the ***Server***, refer to **Appendix B. Server Credentials**.

6.1 General Tab

Use the **General** tab to name the ***Server*** and provide paths to required directories.

Optim Server

The name (1 to 15 characters) of the ***Server***. If you do not provide a name, the computer name is the default.

Note: The ***Server*** name must be added to the Product Configuration File for your site.

Temporary Work Directory

The complete path to the default directory in which you want the ***Server*** to store internal work files and trace files. To select from system directories, click the browse button. This directory must be unique to the ***Server*** and different from the Temporary Work Directory specified in Personal Options.

Data Directory

The complete path to the default directory in which you want the ***Server*** to store process files for which an explicit directory path is not provided. To select from your system directories, click the browse button. This directory must be unique to the ***Server*** and different from the Data Directory specified in Personal Options.

Create a subdirectory within the Data Directory for clients

Select **Create a subdirectory within the Data Directory for clients** to automatically create a subdirectory in the ***Server*** data directory, when each workstation first connects to the ***Server***. The new subdirectory becomes the default data directory for the workstation. The name of the new subdirectory is determined by the Windows Logon name from the workstation.

For example, if this option is selected and the data directory is D:\DATA when user "JOHN" connects to the ***Server***, the subdirectory D:\DATA\JOHN becomes the default data directory for JOHN.

Maximum Processes

Use **Maximum Processes** to limit the number of simultaneous processes that can run on the ***Server***. Specify the limit according to the capacity of the ***Server*** machine (CPU, disk space, network access speed, memory, etc.). Valid values are from 10 to 48. The default value is 48. When the server reaches the maximum, an error message (**Server too Busy**) is displayed.

Typically, one validation process, called a Mirror, is created each time a Request Editor that requires the ***Server*** is opened. When the request is run, a Mirror and the request process simultaneously. Therefore, two processes run for each request. (For example, if a workstation delegates two requests to the ***Server*** simultaneously, four processes are used.)

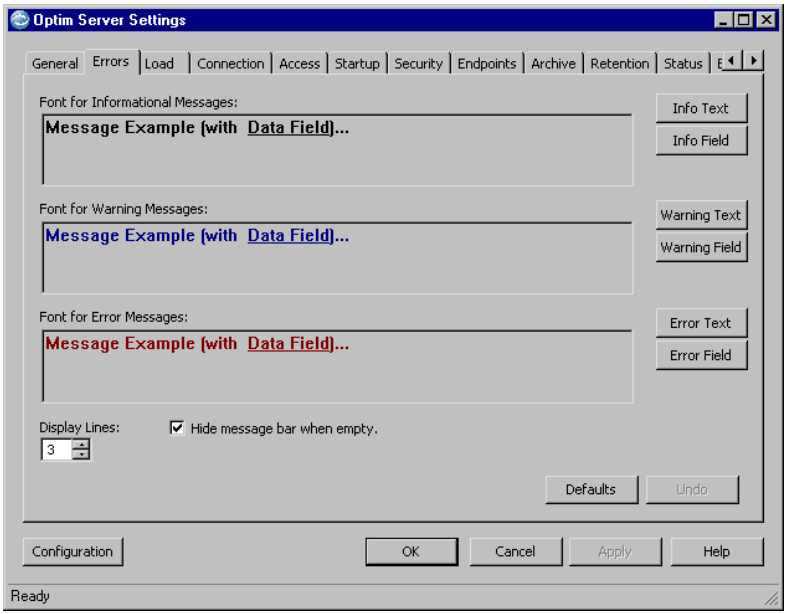
Days to keep Trace files

The number of days (2 to 30) to retain trace files in the temporary work directory. The default value is 5.

Trace files are useful for tracking the processing performed using ***Optim***. Trace file names are prefixed with PR0, followed by letters indicating the trace file type, ended with a numeric extension (for example, PR0TOOL.123). The extension on the name of the trace file distinguishes one trace file of that type from another. Trace files are sequentially numbered .001 through .999, followed by .A00 through .Z99, as necessary. If more than 3,599 trace files of a single type are created and stored within the specified number of days, file names are reused, beginning with the first.

6.2 Errors Tab

Use the **Errors** tab to assign default font information for messages.



The default fonts for message text and data fields are shown in each of the font message boxes. To open the Windows **Font** dialog to select font attributes, click the command buttons for text or fields. To modify the font for text messages, click **Text**. To modify the font for data fields noted in message text, click **Field**.

Font for Informational Messages

Informational messages are not critical; for example, messages that ask whether information should be saved when a dialog is closed.

Info Text — Specify font characteristics for the informational message text. The default is System, 10 point, Bold, Black.

Info Field — Specify font characteristics for the data referenced in an informational message. The default is System, 10 point, Bold, Underline, Black.

Font for Warning Messages

Warning messages indicate serious, but not critical conditions. A warning message does not interrupt an action, but may indicate that you should reevaluate the current action.

Warning Text Specify font characteristics for the warning message text. The default is System, 10 point, Bold, Navy.

Warning Field Specify font characteristics for the data referenced in a warning message. The default is System, 10 point, Bold, Underline, Navy.

Font for Error Messages

Error messages indicate critical conditions and interrupt the current action. A problem presented in an error message must be addressed before the attempted action can proceed. Error messages can appear in pop-up dialogs, but usually display in the message bar at the bottom of a dialog.

Error Text Specify font characteristics for the error message text. The default is System, 10 point, Bold, Maroon.

Error Field Specify font characteristics for the data referenced in an error message. The default is System, 10 point, Bold, Underline, Maroon.

Display Lines

Specify the maximum number of lines (3 to 9) to display in the message bar for any type of message.

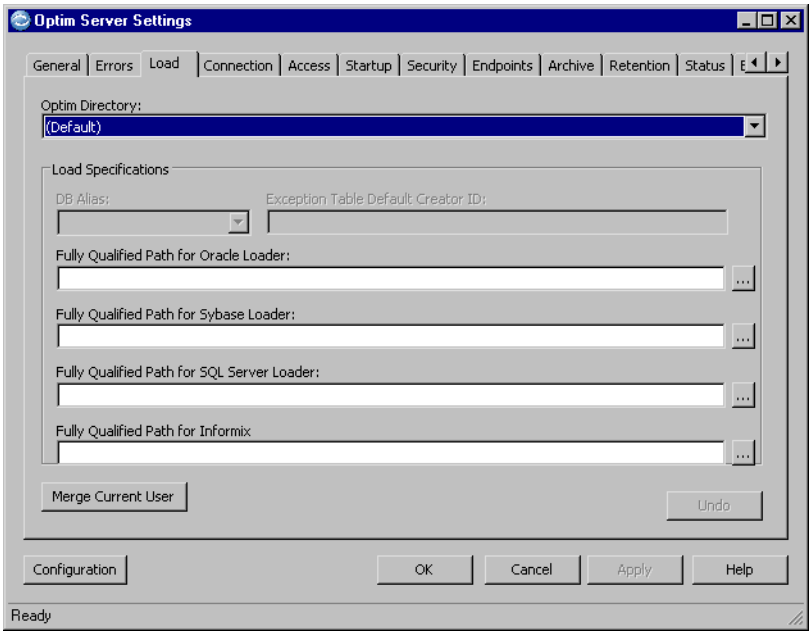
Hide message bar when empty

Select this check box to hide the message bar when no informational, warning, or error messages are displayed. If you clear this check box, the message bar appears at the bottom of each editor or dialog even when empty.

6.3 Load Tab

Use the **Load** tab to specify the paths to DBMS loaders:

Note: You can expedite the configuration of the Load settings for the ***Server*** by clicking **Merge Current User**. This merges Load settings for the logged-on user in the Current User registry with settings for the ***Server*** machine in the Local Machine registry.



***Optim* Directory**

Select [Default] in the **Optim Directory** list to enter the path and name of the Loader executable file for each DBMS type.

If you have more than one version of a particular DBMS type, you can enter the unique loader specification for each version. Select the specific ***Optim*** Directory and DB Alias, then enter the appropriate path and name of the Loader executable file for the particular DBMS version.

Load Specifications

Specify the complete path and name of the executable to access each DBMS Loader that can be used with a Load Request.

DB Alias	Select a specific ***Optim*** Directory, then click the down arrow to select a specific DB Alias. Specify the appropriate loader path for the corresponding DBMS version. If you are using DB2, Oracle, or Informix, you can also specify a default Creator ID for Exception Tables (or Violation Tables).
Exception Table Default Creator ID	Specify a default Creator ID for exception tables (DB2 and Oracle) or violation tables (Informix). (Available only when you select a DB Alias for a DB2, Oracle, or Informix database.)
Fully Qualified Path for DBMS Loaders	Specify the directory path and program name for the specific DBMS Loader. Consult your DBMS documentation for the name of the loader program. To select from your system directories, click the browse button.

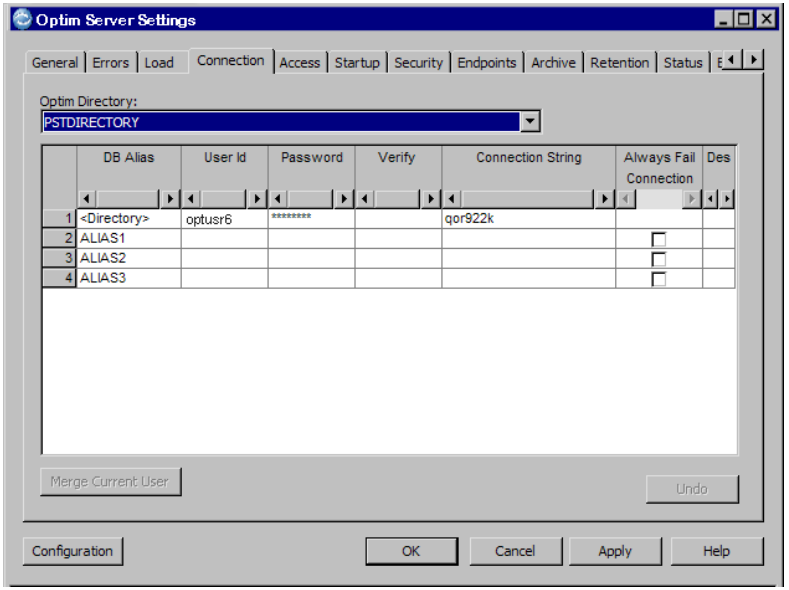
Merge Current User

Click **Merge Current User** to merge the settings from the Current User registry to the Local Machine registry for the ***Server*** machine.

6.4 Connection Tab

Use the **Connection** tab to provide DBMS connection information for all DB Aliases in any ***Optim*** Directory required to perform delegated tasks.

Note: You can expedite the configuration of the Connection settings for the ***Server*** by clicking **Merge Current User**. This merges the Connection settings for the logged-on user in the Current User registry with settings for the ***Server*** machine in the Local Machine registry.



Settings on the **Connection** tab and the **Security** tab are related: on the **Security** tab, you choose **Server** or **Client** to specify the source of the User ID and Password information for ***Optim*** Directory and DB Alias access.

- If you select **Server** on the **Security** tab, the appropriate User ID and password entered on the **Connection** tab are used; the User ID and password from the workstation originating the task are not used.
- If you select **Client** on the **Security** tab, the User ID and password from the workstation originating the task are used.

Note: The **Connection String** information you enter on the **Connection** tab is used regardless of whether you select **Server** or **Client** on the **Security** tab. Leave the connection string blank, or select the **Always Fail Connection** check box to prevent the ***Server*** from accessing an ***Optim*** Directory and/or DB Alias when performing delegated tasks.

Optim Directory

Select an ***Optim*** Directory from the list to display the connection information for the corresponding DB Aliases.

Grid Details

The connection information for the selected ***Optim*** Directory includes the following:

Note: The maximum length for a User ID or password varies by DBMS.

DB Alias — DB Aliases in the selected ***Optim*** Directory.

User ID — Identifier (1 to 30 characters) that allows the ***Server*** to use a particular DB Alias. User IDs are usually assigned and maintained by the database administrator.

Note: If you are using Informix, you must enter the User ID in uppercase for an ANSI database and in lowercase for a non-ANSI database.

Password — Enter a password (1 to 30 characters) that allows the ***Server*** to access a database using the specified DB Alias.

Verify — Reenter the password for verification.

Connection String — Connection string the ***Server*** uses to access a database using the specified DB Alias.

Always Fail Connection — Select this check box to deny access to the corresponding DB Alias. You can use this check box to temporarily deny access to a DB Alias without having to remove the connection string.

Description — Text that describes or explains the purpose of the logon record.

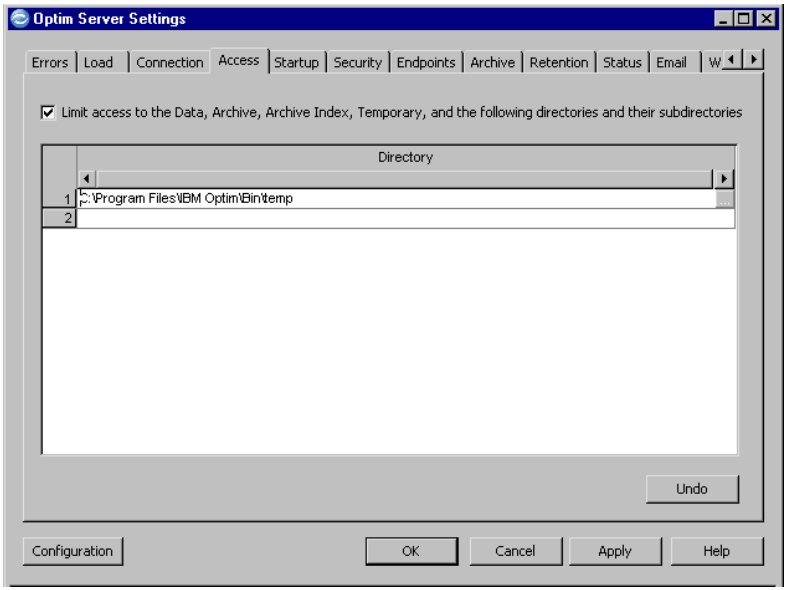
Merge Current User

Click **Merge Current User** to merge the Connection settings from the Current User registry to the Local Machine registry for the ***Server***

component machine. This action does not overlay information previously entered into the **Optim Server Settings** dialog. This action only merges new settings from the Current User. If the settings are the same, this command is unavailable.

6.5 Access Tab

Use the **Access** tab to restrict access to all ***Server*** directories and subdirectories, except those you specify. Access to the ***Server*** data directory, Archive Directory, and Archive Index Directory is enabled, by default.



Limit Access...

The **Limit access to only the Data, Archive, Archive Index and the following directories and their subdirectories** check box is intended to restrict access to ***Server*** files and directories, and is selected by default. When this check box is selected, access to the ***Server*** data directory, Archive Directory, and Archive Index Directory is enabled. You can allow access to additional files and directories, by entering each one in the **Directory** grid.

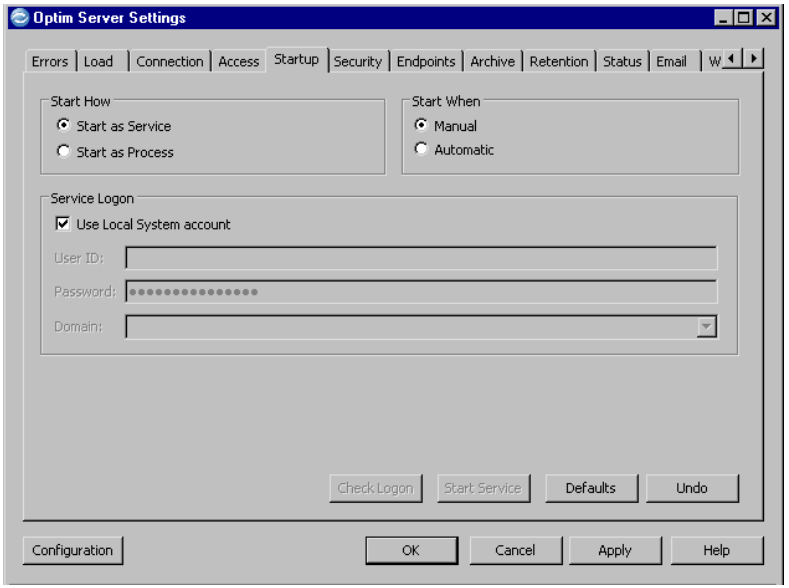
Clear the check box to provide access to all ***Server*** files and directories.

Directory

Enter paths to specific directories and subdirectories accessible to delegating workstations. Click the browse button to select from a list.

6.6 Startup Tab

Use the **Startup** tab to assign startup information.



Start How

Start as Service The ***Server*** is enabled when the machine is started. A service does not need a currently logged on user (the machine can be left unattended).

Note: When the ***Server*** runs as a service, mapped drives are unavailable.

Start as Process The ***Server*** starts in a DOS window. The security of the logged-on user applies; you cannot use a service logon.

Start When

When **Start as Service** is selected:

Manual Only the logged-on user can start the ***Server***. (You can use the **Optim Server Settings** dialog to start the ***Server***.)

Automatic The ***Server*** starts when system boots.

When **Start as Process** is selected:

Manual Select ***Optim*** from the Windows Start Menu.

Automatic When ***Optim*** starts, ***Optim*** is added to the Start/Startup menu.

Service Logon

When **Start as Service** is selected, you must provide service logon information.

Use Local System account Select this check box to use the logon information for the local machine, as provided on the Personal Options **Server** tab.

If you clear this check box, you must provide explicit credentials, as follows.

User ID Enter the appropriate User ID.

If these **Server** credentials are used to access files external to the **Server**, the User ID must have the following privileges:

- Act as part of the operating system (SeTcbPrivilege)
- Increase quotas (SeIncreaseQuotaPrivilege)
- Replace a process level token (SeAssignPrimaryTokenPrivilege)
- Bypass traverse checking (SeChangeNotifyPrivilege)

For more information about these privileges, refer to **B.1.3 Server Privileges for Explicit or Client Credentials** on page 422.

Password Enter the password corresponding to the User ID.

Domain Specify the domain.

Check Logon

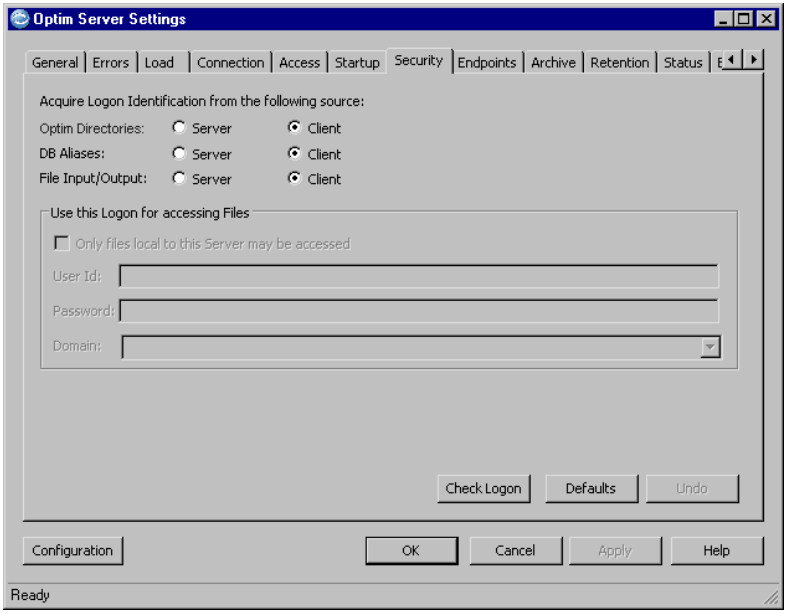
Click **Check Logon** to verify that the ***Server*** can log on with the credentials provided. This button is available if the **Use Local System account** check box is cleared.

Start/Stop Service

This button is available if **Start as Service** is selected and applied.

6.7 Security Tab

Use the **Security** tab to choose the source of the logon information for the ***Server***.



Select options to indicate the source of the logon information when the ***Server*** requires access to ***Optim*** Directories, DB Aliases, and Input and Output files.

Optim Directories

Server Select to use the User ID and password provided on the **Connection** tab for ***Server*** access to the ***Optim*** Directory.

Client Select to use the User ID and password for ***Server*** access to the ***Optim*** Directory, as provided in Personal Options for the delegating workstation. (In Personal Options, you can also require a password each time, or deny access. Refer to **9.2.9 Server Tab** on page 305 for more information.)

DB Aliases

Server Select to use the User ID and password provided on the **Connection** tab for ***Server*** use of DB Aliases.

Client Select to use the User ID and password for ***Server*** use of DB Aliases, as provided in Personal Options on the delegating workstation. (In Personal Options, you can also require a password each time, or deny access. Refer to **9.2.9 Server Tab** on page 305 for more information.)

File Input/Output

Server Select to use the **Service Logon** on the **Startup** tab. This setting applies only when **Server** credentials are used for file access.

Client

- Select this option to use User ID, password, and domain specified on the **Server** tab in Personal Options on the delegating workstation for ***Server*** local disk and network share access. Refer to **9.2.9 Server Tab** on page 305 for more information.

The delegating credentials must have the following privilege.

- Log on as a batch job (SE_BATCH_LOGON_NAME

(Note that, in some installations, you can give this privilege to everyone in the Local Security Policy, instead of specifying credentials for each user.)

Use this Logon for accessing files If files are accessed using ***Server*** credentials, you must indicate the source of those credentials.

Only files local to this Server may be accessed Select **Only files local to this Server may be accessed** to restrict ***Server*** access to local files. Clear the check box to provide Logon information needed for ***Server*** access to files.

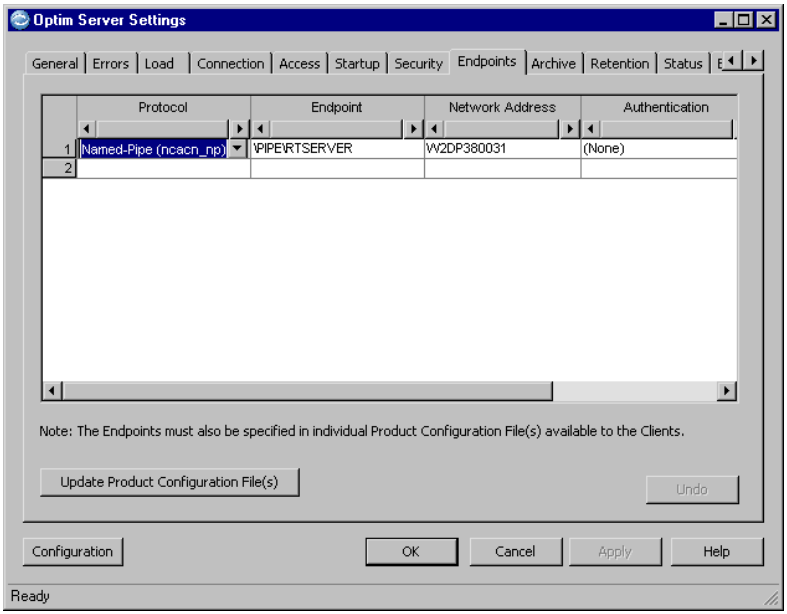
User ID	Enter the appropriate User ID. If these credentials are used to access files external to the **Server**, the User ID must have the following privileges: • Act as part of the operating system (SeTcbPrivilege) • Increase quotas (SeIncreaseQuotaPrivilege) • Replace a process level token (SeAssignPrimaryTokenPrivilege) • Bypass traverse checking (SeChangeNotifyPrivilege) • Log on as a batch job (SE_BATCH_LOGON_NAME
Password	Enter the password corresponding to the User ID.
Domain	Specify the domain.

Check Logon Click **Check Logon** to verify that the ***Server*** can log on with the credentials provided.

6.8 Endpoints Tab

Use the **Endpoints** tab to specify protocols to be used by workstations connecting to the ***Server*** for remote procedure calls.

The protocol **Named-Pipe (ncacn_np)** and endpoint **\PIPE\RTSERVER** are entered by default. This is usually the most efficient method for workstations in the domain to connect to the ***Server***. To add access for a workstation outside the domain, you must add the additional protocol.



You can include all protocols and endpoints available to the ***Server*** by clicking the down arrow in **Protocol** and selecting **Supported Protocols (All)** from the list. Endpoints are created for every available protocol. When configured this way, workstations must query an RPC Locator for the endpoints when connecting to the ***Server***. This query introduces a small delay when the server is first selected and may compromise security.

Note: When **Supported Protocols (All)** is selected, **Endpoint** displays an asterisk (*) and **Network Address** displays the computer name.

Grid Details

Protocol	Click the down arrow to select from a list of available protocols.
Endpoint	Specify the endpoint, or address, that corresponds to the specified protocol. (The format and content depend on the specified protocol.)
Network Address	Displays the network address of the ***Server***. (The format and content depend on the specified protocol.)
Authentication	In selecting a level of security, the needs of your site must be weighed against potential performance compromises. • The higher the protection level, the greater the overhead required. • The more often verification is requested, the more time required to complete a process. Select the appropriate level of authentication.

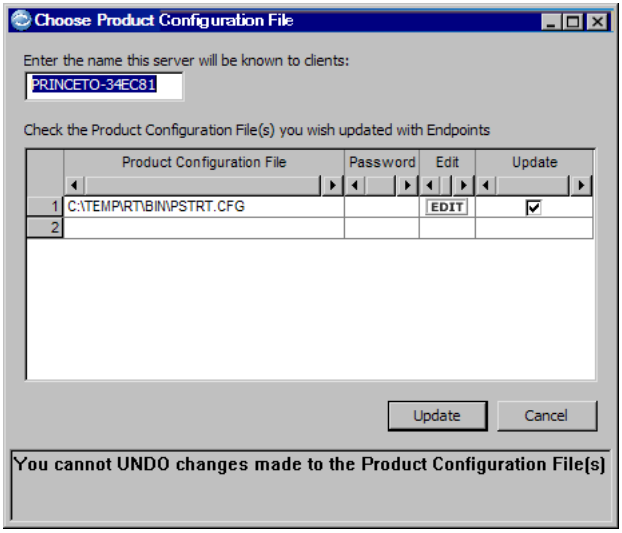
None	No authentication is required.
During Connect (first call only)	Authenticate when the user connects to the ***Server*** on the first call. This security level ensures only that the connection is valid and is from the proper user. No further authentication is made and transferred data is not verified. This level of security requires the least overhead and, of the available options, offers the least security.
Every Call	Authenticate the user each time data is exchanged, regardless of number of packets.
Each Packet	Confirm that each packet of transferred data is received from the authenticated user. This level of security requires more overhead and offers more protection than the Connect Level.

Each Packet (Verify not changed)	Confirm that each packet of transferred data is received from the authenticated user and verify that it has not been modified. This level of security requires more overhead and offers more protection than the Packet Level.
Each Packet (Verify not changed and Encrypt)	Confirm that each packet of transferred data is received from the authenticated user, verify that it has not been modified, and encrypt the argument value of each remote procedure call. This level of security requires the most overhead and, of the available options, offers the most protection.

Update Product Configuration Files

Each workstation to connect to the ***Server*** must use a Product Configuration File that includes ***Server*** endpoint information. The Product Configuration File used by a workstation is specified in Personal Options.

To update Product Configuration Files with new information entered on the **Endpoints** tab, click **Update Product Configuration File(s)**. Use the **Choose Product Configuration File** dialog to list Product Configuration Files to update.



Note: If a Product Configuration File to be updated is unavailable from the **Choose Product Configuration File** dialog, the file must be updated manually on the corresponding workstation.

Enter the name this server will be known to clients

Enter a name for the ***Server***. The name you enter is added to the list of available ***Servers*** displayed in action request editors that can use a ***Server*** for remote processing.

Grid Details

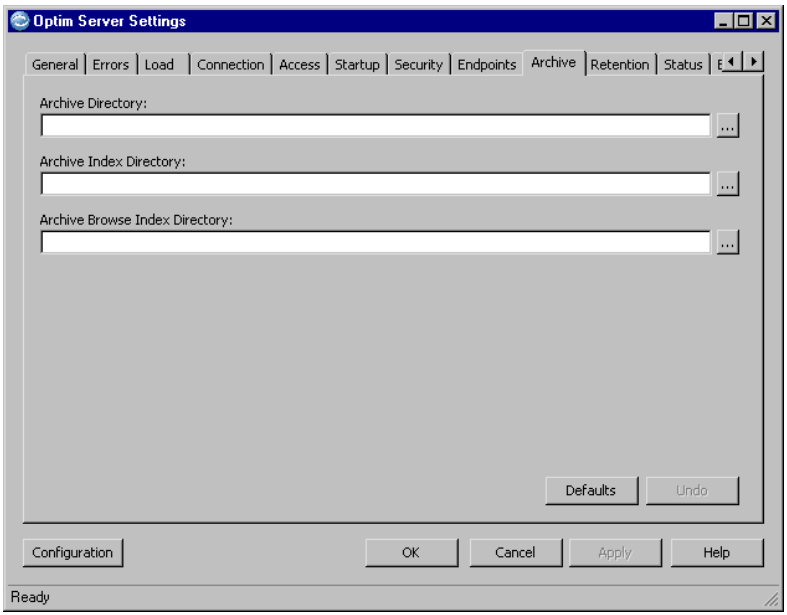
Product Configuration File	Specify the complete path to each Product Configuration File to be updated. To select from your system directories, click the grid cell and click the browse button. Each time you enter a Product Configuration File, you are prompted for the corresponding password. The password is set in Product Options.
Password	When you enter the password for a Product Configuration File the first time, the password is saved for future updates to the Product Configuration File. For security reasons, the password displays as a series of asterisks (****).
Edit	Click **Edit** to display the **Product Options Editor** for the corresponding Product Configuration File.
Update	Select the check box to include the corresponding Product Configuration File to be updated.

Update

Click **Update** to update each selected Product Configuration File with the new endpoint information.

6.9 Archive Tab

Use the **Archive** tab to enter the path to the default Archive, Archive Index, and Archive Browse Index Directories for the ***Server***.



Archive Directory

Specify the complete path to the default directory where you want the ***Server*** to store Archive Files. To select from your system directories, click the browse button. If you do not specify a directory, the Data Directory specified on the **General** tab is used by default.

Archive Index Directory

Specify the complete path to the default directory where you want the ***Server*** to store Archive Index Files. To select from your system directories, click the browse button. If you do not specify a directory, the Archive Directory is used by default.

Archive Index Browse Directory

Specify the complete path to the default directory where you want the ***Server*** to store Archive Index Browse Files. To select from your system directories, click the browse button. If you do not specify a directory, the Archive Directory is used by default.

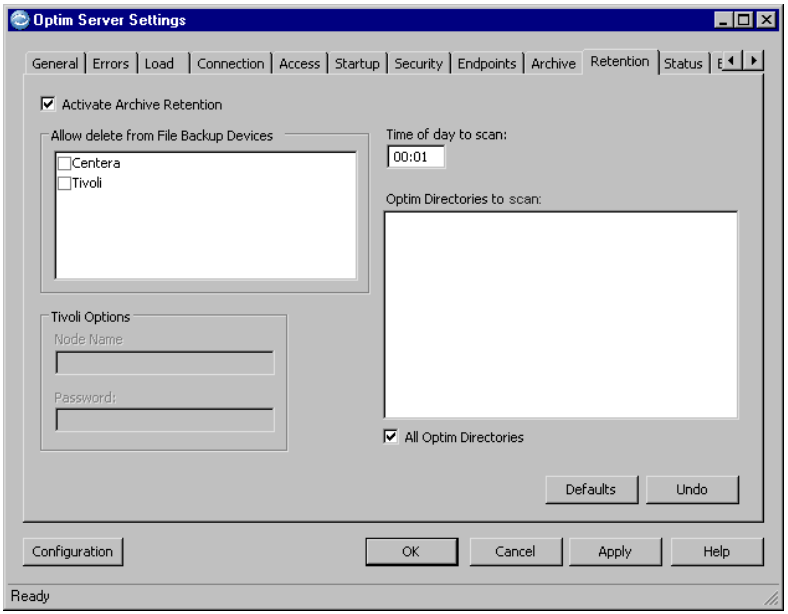
An Archive Index Browse File is created automatically whenever you join tables while browsing an Archive File. The Archive Index Browse File stores primary key and foreign key information to expedite the

retrieval of data, and has an *.abf* extension, by default. Archive Index Browse Files are dynamically updated, so it is advisable to select a directory accessible to any user that may browse an Archive File.

6.10 Retention Tab

A retention policy allows you to automatically delete Archive Files that reside on the ***Server***. When Archive Retention is activated, the ***Server*** scans ***Optim*** Directories for Archive Files with a retention policy. The **Retention** tab allows you to activate Archive retention, select the ***Optim*** Directories to scan, the time of day to scan, and configure options for deleting Archive Files from File Backup Devices (e.g., EMC Centera, HP RISS, and IBM Tivoli®).

For more information about specifying a retention policy, see the ***Archive*** **User Manual, 10.2.8 Retention Policy Tab.**



Activate Archive Retention

Select this check box to scan the selected ***Optim*** Directories. If you clear the check box, the ***Optim*** Directories are not scanned, but the parameters on the **Retention** tab remain.

Allow delete from File Backup Devices

List of the Backup Devices integrated with ***Archive***. Select the appropriate check box(es) to allow the device to delete the Archive File when the retention policy has elapsed.

Tivoli Options

Specify the node name and password that allow the ***Server*** to access the Tivoli tape backup device.

Note: To use a Tivoli device, you must install the Tivoli client and API support on the machine where the ***Optim Server*** runs.

Node Name Identifier needed to access the Tivoli tape backup device.

Password Password needed to access the Tivoli tape backup device.

Note: For security reasons, the password is displayed as a series of asterisks (****).

Time of day to scan The time to begin scanning the ***Optim*** Directories. Use 24-hour time format, for example 1:30 p.m. is 13:30.

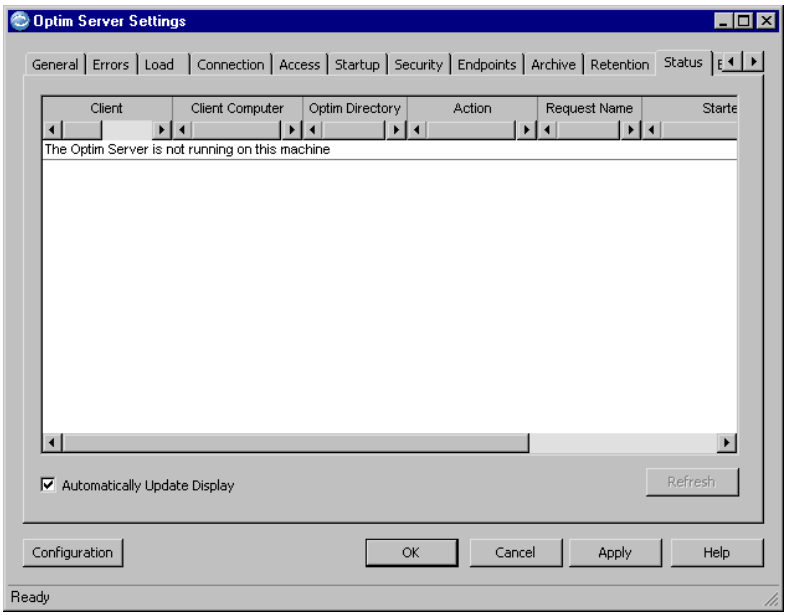
Optim Directories to scan ***Optim*** Directories registered with the ***Server***. Select the ***Optim*** Directories to scan for Archive Files with a retention policy.

All Optim Directories Select to automatically scan all ***Optim*** Directories registered with the ***Server***.

Note: Selecting this option also ensures that any future ***Optim*** Directories registered with the ***Server*** are scanned.

6.11 Status Tab

The **Status** tab displays the current connections to the ***Server***.



Grid Details

The following details display in the grid.

Client	The sign-on user name for the user.
Client Computer	The network computer name for the computer.
Optim Directory	The name of the ***Optim*** Directory in which the request resides.
Action	The type of action that is running.
Request	Displays the fully qualified name of the request that is running, or “Mirror” to indicate the validation processing associated with the action that is running.
Started	The date and time the action started.
Duration	The duration of the connection.

Automatically Update Display

Select this check box to automatically update (refresh) the display whenever a connection is established or broken, and update the **Duration** column in the grid every minute.

Refresh

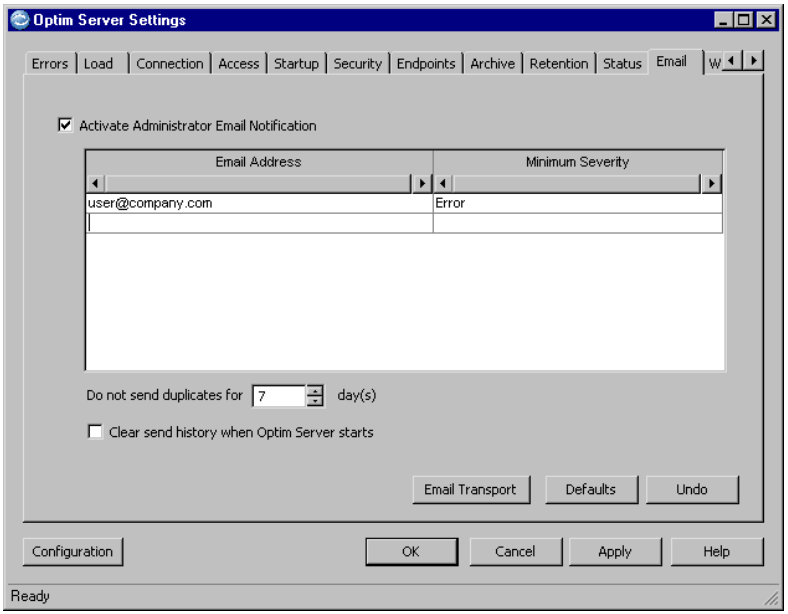
Select **Refresh** to update the display on demand. (**Refresh** is unavailable when the **Automatically Update Display** check box is selected.)

Note: You can right-click on a row and choose **Cancel Request** to cancel the specific connection with the workstation, or **Cancel all for Client** to cancel all connections with the workstation.

6.12 Email Tab

The **Email** tab allows you to automatically send "logged" messages generated by the ***Server*** to the listed email addresses. The ***Server*** sends messages that are reported to the Windows Event Log (for Windows) or the syslog (for UNIX or Linux).

Note: Before using administrator email notification, the desired email program must be installed. For Windows, the email client must be defined as the default, and set up to interface with MAPI. For UNIX or Linux, a valid copy of SENDMAIL must be configured correctly.



Activate Administrator Email Notification

Select this check box to activate email notification. The other options on this tab are unavailable unless this check box is selected.

Note: Deselecting the check box does not clear the **Email** tab settings.

Email Address

Enter an email address to which to automatically send notification. A message is sent to the email address only if the specified Minimum Severity is reached.

Minimum Severity

For each email address you list, select the minimum severity needed to send a message. The severity levels are ranked from least severe (**Success**) to most severe (**Exception**). Click the down arrow to display a drop-down list with the following severity levels:

Success	Send email notification for all processing messages including **Success.**
Information	Send email notification for **Information** or more severe messages.
Warning	Send email notification for **Warning** or more severe messages.
Error	Send email notification for **Error** or more severe messages.
Exception	Send email notification for **Exception** messages.

To clear entries, right-click a grid cell and select **Remove** or **Remove All** from the shortcut menu.

Do not send duplicates for ... day(s)

Specify the number of days (1 to 999) before email notification is resent for a persistent error or warning.

Clear send history when Optim Server starts

Select this check box to clear the send history once the ***Server*** is started. When selected, any email notification that took place prior to the starting of the ***Server*** is ignored.

Send Test eMail

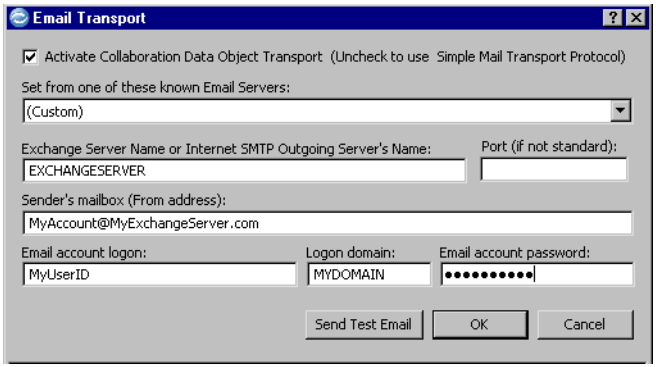
Right-click a grid row and select **Send Test eMail** to validate the email address.

Email Transport

Click this button to display the **Email Transport** dialog so that you may activate and configure the Collaboration Data Object (CDO) transport to send email. If you don't click this button, email is sent using the Simple Mail Protocol Transport (SMTP).

Note: You must use the CDO transport if the email client on the server requires logon credentials to send an unattended message or requires user input when SMTP is used to send a message. Also, select the CDO option if the server uses a

Microsoft Outlook client (version 2000 or later) to send messages through a Microsoft Exchange server.



Activate Collaboration Data Object Transport

If you use the SMTP email transport, keep this check box cleared (default) and select **OK**. A popup will ask you if you want to connect without entering a password. If you use the CDO email transport, select this check box to enable the dialog and continue entering information.

Set from one of these known Email Servers

Click to select an account from the list and populate the remainder of the **Email Transport** dialog with information for the selected account.

Exchange Server Name or Internet SMTP Outgoing Server's Name

Type an exchange server name or internet address.

Port (if not standard)

Type a port name or leave blank (default port).

Sender's mailbox (From address)

Type the sender (From) email address.

Email account logon

Type the email logon name.

Logon domain

Type the domain name.

Email account password

Type the password. A blank password is valid if the account allows it; a prompt will confirm that you want to connect without entering a password.

Send Test Email

Click this button to send a test email to your mailbox.

Note: It is recommended that you send a test email to ensure that the information you entered is sufficient to send an email. If you

do not receive the test email, make the necessary corrections to the information you entered.

6.13 Conclusion

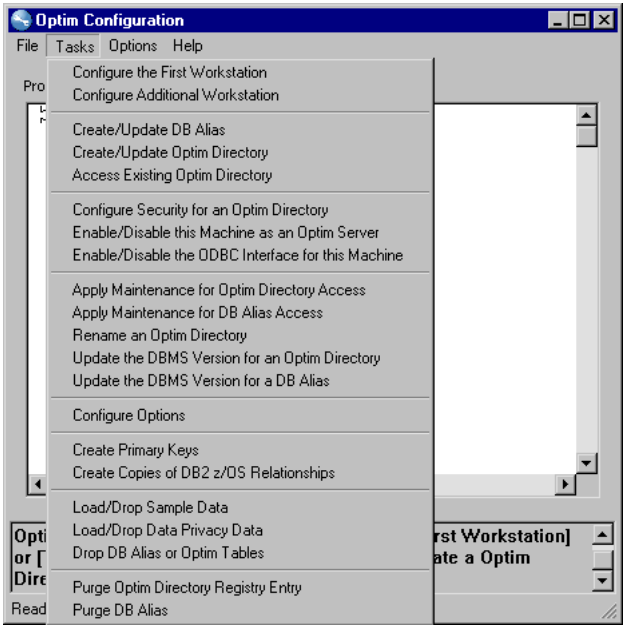
After you configure the first workstation, any additional workstations, and any ***Servers***, you are ready to start using ***Optim***.

Note: If you make changes to the configuration of a ***Server*** while it is running, click **Apply**, then stop and start the ***Server*** to effect the changes.

The remaining sections explain how to use the various other commands available from the **Tasks** menu of the **Configuration** program.

7. Maintenance and Other Configuration Tasks

After you configure the first and any additional workstations, you are ready to start using ***Optim***. However, periodically, it may be necessary to perform other tasks that are available from the **Tasks** menu.


Optim Configuration
File
Tasks
Options
Help
Configure the First Workstation
Configure Additional Workstation
Create/Update DB Alias
Create/Update Optim Directory
Access Existing Optim Directory
Configure Security for an Optim Directory
Enable/Disable this Machine as an Optim Server
Enable/Disable the ODBC Interface for this Machine
Apply Maintenance for Optim Directory Access
Apply Maintenance for DB Alias Access
Rename an Optim Directory
Update the DBMS Version for an Optim Directory
Update the DBMS Version for a DB Alias
Configure Options
Create Primary Keys
Create Copies of DB2 z/OS Relationships
Load/Drop Sample Data
Load/Drop Data Privacy Data
Drop DB Alias or Optim Tables
Purge Optim Directory Registry Entry
Purge DB Alias

For example, to expand the number of databases, you can create or update a DB Alias, apply maintenance for DB Alias access, or update the version of the DBMS. Similarly, you can create an additional ***Optim*** Directory, apply maintenance for ***Optim*** Directory access, or update the version of the DBMS for an ***Optim*** Directory. You can also select options to purge a DB Alias or purge an ***Optim*** Directory registry entry.

Other tasks include configuring Product and Personal Options, creating primary keys, and creating copies of DB2 z/OS relationships to be used in ***Optim***. You may also load or drop the sample data included with ***Optim***; this data provides a starting point for using many features in ***Optim***. If you have a Data Privacy License, you may also load and drop the data privacy data tables provided with ***Optim***. You may also choose to drop a DB Alias or ***Optim*** Directory Tables as well as enable or disable the ***Optim*** Security features. Each task is described in the following sections.

7.1 Create/Update DB Alias

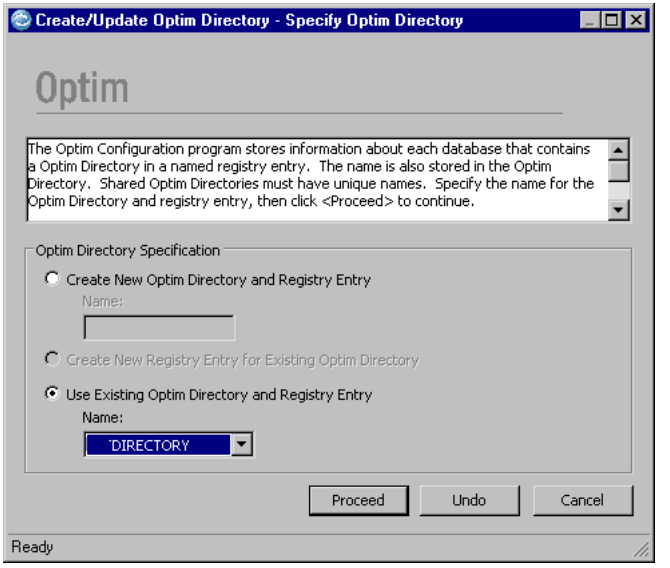
Optim supports the use of any number of database instances. However, there must be a unique DB Alias in the active ***Optim*** Directory for each database instance. A DB Alias serves as a high-level qualifier for naming database tables and provides a single name for connecting to a particular database. You can define the necessary DB Aliases at installation, or use the **Configuration** program to add DB Aliases after installation by selecting **Configuration Assistant** from the **Help** menu or by selecting **Create/Update DB Alias** from the **Tasks** menu.

Notes:

- If using the ***Server*** to access data referenced by the DB Alias, you also must add the DB Alias information to the **Connections** tab on the **Optim Server Settings** applet. See **Chapter 6. Configure the Optim Server**.
- If Object Security is enabled and DB Alias objects are secured when saved, a new DB Alias is secured by an ACL modeled after the ***Optim*** Object Template ACL. If the ***Optim*** Object Template ACL has not been defined when you create a DB Alias, you must define an ACL for each object that requires an ACL. For more information about securing objects, see **D.2 Access Control List** on page 469.

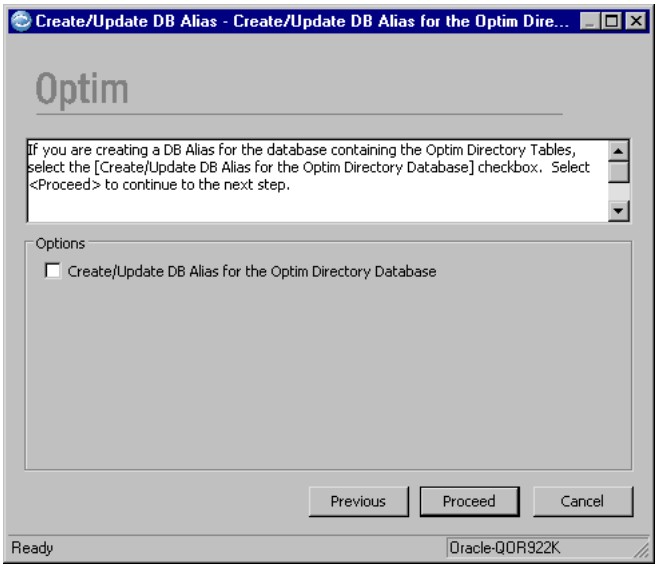
Specify Optim Directory

The first step in creating a new DB Alias is to specify the ***Optim*** Directory where you want to store that DB Alias. The **Configuration** program displays the **Specify Optim Directory** dialog.


Create/Update Optim Directory - Specify Optim Directory
Optim
The Optim Configuration program stores information about each database that contains a Optim Directory in a named registry entry. The name is also stored in the Optim Directory. Shared Optim Directories must have unique names. Specify the name for the Optim Directory and registry entry, then click <Proceed> to continue.
Optim Directory Specification
Create New Optim Directory and Registry Entry
Name:
Create New Registry Entry for Existing Optim Directory
Use Existing Optim Directory and Registry Entry
Name:
DIRECTORY
Proceed
Undo
Cancel
Ready

The option to **Use Existing Optim Directory and Registry Entry** is selected. Specify the name of the ***Optim*** Directory you want to use. To select from a list, click the down arrow. To continue, click **Proceed**.

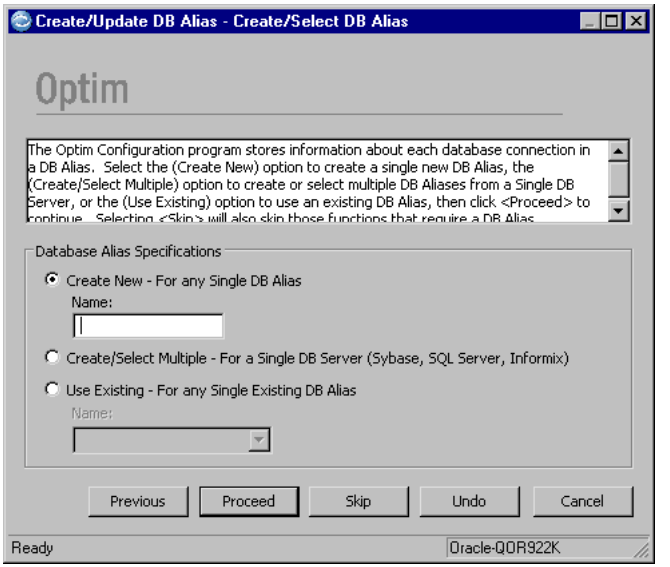
The **Configuration** program opens a query dialog.


Create/Update DB Alias - Create/Update DB Alias for the Optim Dire...
Optim
If you are creating a DB Alias for the database containing the Optim Directory Tables, select the [Create/Update DB Alias for the Optim Directory Database] checkbox. Select <Proceed> to continue to the next step.
Options
Create/Update DB Alias for the Optim Directory Database
Previous
Proceed
Cancel
Ready
Oracle-QOR922K

If you plan to use ***Optim*** to access user tables (other than ***Optim*** Directory tables) on the database, select the **Create/Update DB Alias for the Optim Directory Database** check box. If you want to create a DB Alias for another database (or server), clear the check box.

Create/Select DB Alias

On the **Create/Select DB Alias** dialog, specify the DB Alias name.


Create/Update DB Alias - Create/Select DB Alias
Optim
The Optim Configuration program stores information about each database connection in a DB Alias. Select the (Create New) option to create a single new DB Alias, the (Create/Select Multiple) option to create or select multiple DB Aliases from a Single DB Server, or the (Use Existing) option to use an existing DB Alias, then click <Proceed> to
Database Alias Specifications
Create New - For any Single DB Alias
Name:
Create/Select Multiple - For a Single DB Server (Sybase, SQL Server, Informix)
Use Existing - For any Single Existing DB Alias
Name:
Previous
Proceed
Skip
Undo
Cancel
Ready
Oracle-QOR922K

From this point, the task is similar to creating a DB Alias when configuring the first workstation. For details, see **5.1.3 Create DB Aliases** on page 94.

You specify the DB Alias DBMS and then connect to the database (**User ID**, **Password**, and **Connection String**). You also create or update the DB Alias, packages, plans, or procedures. The following guidelines apply:

- If you update an existing DB Alias and you specify a valid connection string or qualifier (for packages, plans or procedures) that differs from the one associated with the DB Alias, you are prompted to update the DB Alias.
- If you attempt to create a DB Alias for a database that has the same signature as an existing DB Alias, the **Configuration** program displays a warning message.
- For Sybase ASE or SQL Server, if you intend to convert existing DB Aliases to use shared stored procedures, select the **Create/Select Multiple** option.
- For SQL Server, if you selected to create/select multiple DB aliases, the User ID must have database owner (dbo) privileges.

After you create the DB Alias, you can create ***Optim*** Primary Keys and Load the Sample Tables included with ***Optim***. If you have a Data Privacy License, you may also load and drop the Data Privacy Data Tables provided with ***Optim***. The **Configuration** program then prompts you to create or update DB Aliases for other databases and repeats the process. Otherwise, the process completes and returns to the main window.

7.2 Create/Update *Optim* Directory

Optim supports using one or several ***Optim*** Directories; however, each workstation can use only one ***Optim*** Directory at a time. In other words, a workstation cannot access information in one ***Optim*** Directory while using ***Optim*** with a different ***Optim*** Directory. Each ***Optim*** Directory must have unique DB Aliases for the databases used with ***Optim*** and unique identifiers for the packages, plans, or procedures associated with the databases.

In most cases, a site uses only one ***Optim*** Directory that is created when the first workstation is configured. However, you may create an additional ***Optim*** Directory as a step in re-locating the ***Optim*** Directory or when a new Directory is required by an upgrade to ***Optim***.

For example, if a site were to have an ***Optim*** Directory in an Oracle database and decided to move it to a DB2 database, the administrator could export a copy of the ***Optim*** objects in the Oracle database to an external file. The administrator would then create the second ***Optim*** Directory in the DB2 database, and import the ***Optim*** objects before dropping or disabling the original ***Optim*** Directory.

Creating an additional ***Optim*** Directory is similar to creating an ***Optim*** Directory when configuring the first workstation. First, you create the ***Optim*** Directory. Then, you create DB Aliases and configure the databases to be used with ***Optim*** when linked to the ***Optim*** Directory. Next, you create or specify the Product Configuration File and modify Personal and Product Options, as needed. You can also initialize ***Optim*** Security for the ***Optim*** Directory. For complete information on creating an ***Optim*** Directory, refer to **5.1.2 Create Optim Directory** on page 78.

7.3 Access Existing *Optim* Directory

A workstation uses a Windows registry entry to access the ***Optim*** Directory. This registry entry is typically created when the workstation is configured, however, if a workstation must access more than one ***Optim*** Directory, you must create entries for each ***Optim*** Directory after the first.

The task to **Access Existing Optim Directory** replicates the steps described in **5.2.2 Create Registry Entry** on page 143. You must specify the ***Optim*** Directory and the DBMS Type and Version for the database where the ***Optim*** Directory is stored. In addition, you must provide information to connect to the database, including an identifier for ***Optim*** Directory tables. This task does not prompt to create a separate Product Configuration File or to modify Product or Personal Options.

7.4 Configure Security for an *Optim* Directory

To initialize ***Optim*** Security and assign the Security Administrator for the directory, select the **Configure Security for an Optim Directory** option from the **Configuration** program **Tasks** menu. Only one Security Administrator can be assigned to an ***Optim*** Directory. After ***Optim*** Security is initialized, the Security Administrator can use this option to enable or disable Functional Security, Object Security, and Archive File Security.

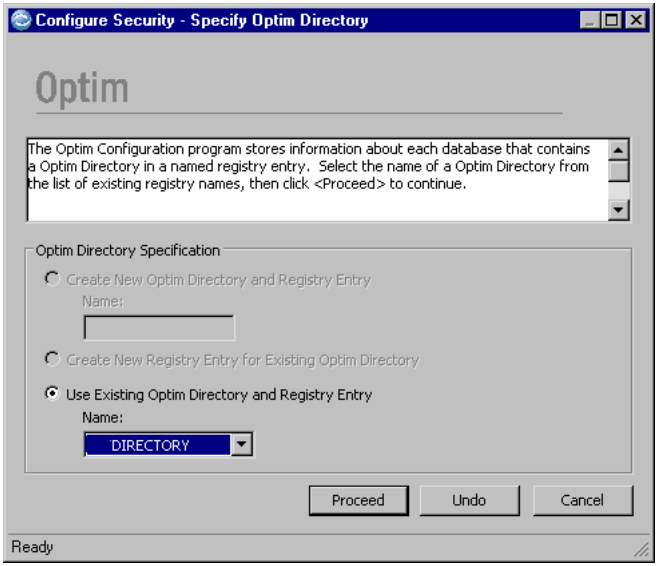
Note: You can also initialize ***Optim*** Security from the following **Configuration** program options: **Configure the First Workstation**, **Create/Update Optim Directory**, and **Configure Options**; however, you can both initialize ***Optim*** Security and enable the security features from the **Configure Security for an Optim Directory** task only.

The Security Administrator can also control access to the **(Default)** Access Control Domain (ACD) and Access Control List (ACL).

7.4.1 Specify *Optim* Directory

When you select **Configure Security for an Optim Directory** from the **Tasks** menu in the **Configuration** program, the **Specify Optim Directory** dialog is displayed. The option to **Use Existing Optim Directory and Registry Entry** is selected. Specify the name of the

Optim Directory you want to use. To select from a list, click the down arrow.


Configure Security - Specify Optim Directory
Optim
The Optim Configuration program stores information about each database that contains a Optim Directory in a named registry entry. Select the name of a Optim Directory from the list of existing registry names, then click <Proceed> to continue.
Optim Directory Specification
Create New Optim Directory and Registry Entry
Name:
Create New Registry Entry for Existing Optim Directory
Use Existing Optim Directory and Registry Entry
Name:
DIRECTORY
Proceed
Undo
Cancel
Ready

When you click **Proceed** and:

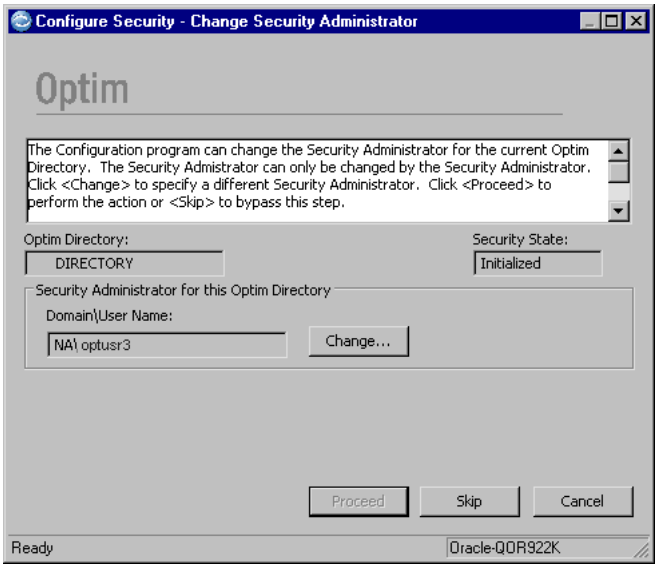
- ***Optim*** Security is not initialized for the Directory, the **Initialize Security** dialog is displayed.
- ***Optim*** Security is initialized, the **Change Security Administrator** dialog is displayed.

7.4.2 Initialize Security or Change Security Administrator

Use the **Initialize Security** dialog to assign a Security Administrator and initialize ***Optim*** Security for the Directory. After security is initialized, the **Set Archive File Security Option** dialog is displayed. For more information about the **Initialize Security** dialog and initializing ***Optim*** Security, see **5.1.4 Optim Security** on page 128.

Use the **Change Security Administrator** dialog to change the Security Administrator for the ***Optim*** Directory. If you do not want to change the

Administrator, click **Skip** to proceed to the **Set Archive File Security Option** dialog.


Configure Security - Change Security Administrator
Optim
The Configuration program can change the Security Administrator for the current Optim Directory. The Security Admistrator can only be changed by the Security Administrator. Click <Change> to specify a different Security Administrator. Click <Proceed> to perform the action or <Skip> to bypass this step.
Optim Directory:
DIRECTORY
Security State:
Initialized
Security Administrator for this Optim Directory
Domain\User Name:
NA\ optusr3
Change...
Proceed
Skip
Cancel
Ready
Oracle-QOR922K

Optim Directory displays the Directory name, and **Security State** indicates that security is *Initialized*. **Security Administrator for this *Optim* Directory** identifies the Security Administrator by the two-part **Domain\User Name**.

Changing the Administrator

To change the Security Administrator, click **Change**. The **Configuration** program displays the next dialog, depending on the following:

- If the Security Administrator is not signed on to the workstation, the **Specify Domain Connection Information** dialog is displayed and the administrator must enter the domain password.
- If the Security Administrator is logged on to the workstation or a password is supplied, the **Specify Domain Connection Information** dialog allows the user to specify a new Security Administrator. For more information, see **Specify Domain Connection Information** on page 129.

After specifying a new Security Administrator, **Security Administrator for this Optim Directory** displays the new Administrator and **Proceed** is available. You must click **Proceed** to complete the change of Administrator.

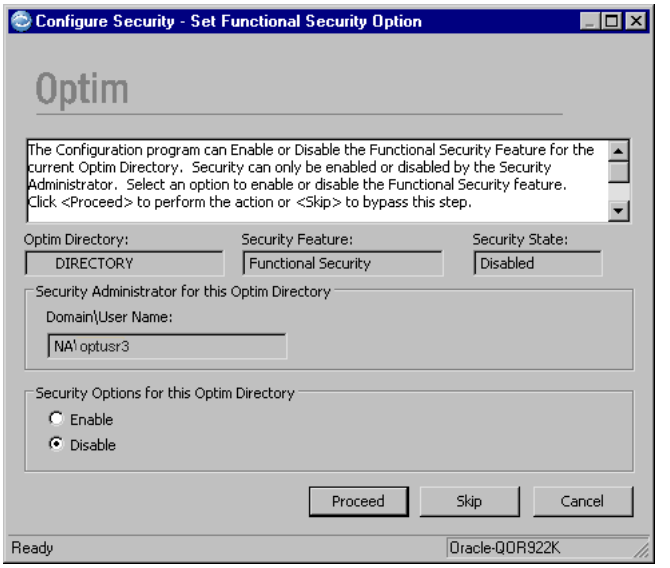
If a new Security Administrator is specified, clicking **Skip** will cancel the change of Administrator.

After clicking **Skip** or **Proceed**, the **Set Archive File Security Option** dialog is displayed.

Click **Cancel** to exit the security configuration process and cancel any changes to the Security Administrator.

7.4.3 Set Functional Security Option

The **Set Functional Security Option** dialog allows the Security Administrator to enable or disable Functional Security for the ***Optim*** Directory. Functional Security controls access to functions and dialogs in ***Optim***. For more information about Functional Security, see **Functional Privileges Tab** on page 458.


Configure Security - Set Functional Security Option
Optim
The Configuration program can Enable or Disable the Functional Security Feature for the current Optim Directory. Security can only be enabled or disabled by the Security Administrator. Select an option to enable or disable the Functional Security feature. Click <Proceed> to perform the action or <Skip> to bypass this step.
Optim Directory:
DIRECTORY
Security Feature:
Functional Security
Security State:
Disabled
Security Administrator for this Optim Directory
Domain\User Name:
NA\ optusr3
Security Options for this Optim Directory
Enable
Disable
Proceed
Skip
Cancel
Ready
Oracle-QOR922K

Optim Directory indicates the directory name, and **Security Feature** shows that Functional Security is the option you can enable or disable. **Security State** indicates that security for the option is Enabled or Disabled. **Security Administrator for this Optim Directory** displays the Security Administrator.

Configuring Functional Security

To enable or disable Functional Security, select **Enable** or **Disable** and click **Proceed**. If the Security Administrator is not signed on to the workstation, the **Specify Domain Connection Information** dialog is displayed and the password for the Security Administrator must be entered.

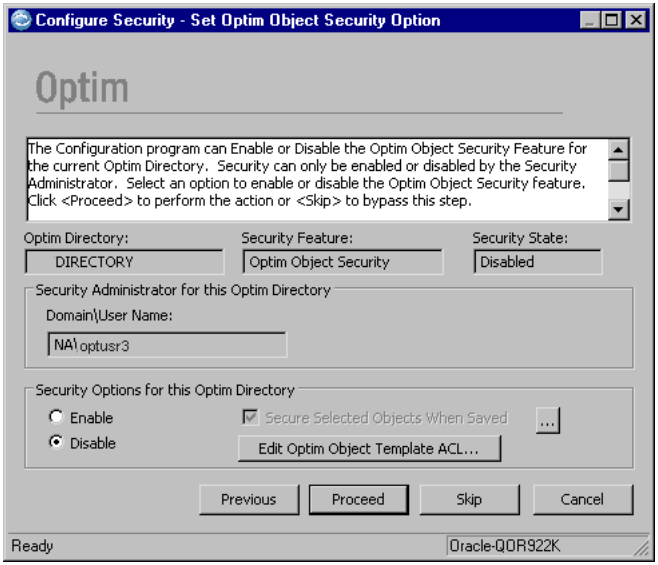
Important: Before Functional Security is first enabled, the Security Administrator must open the **(Default)** ACD and establish Functional Privileges for all users. If Functional Privileges are not defined before Functional Security is enabled, users will be unable to access any functions in ***Optim***. For more

information, see **D.1.1 Access Control Domain Editor** on page 450.

7.4.4 Set Optim Object Security Option

The **Set Optim Object Security Option** dialog allows the Security Administrator to configure Object Security for the ***Optim*** Directory. Object Security controls access to objects in the ***Optim*** Directory such as Column Maps and Access Definitions.

All security definitions are secured by an Access Control List (ACL). Other ***Optim*** objects that have an ACL are secured if Object Security is enabled. For more information about ACLs, see **D.2 Access Control List** on page 469.


Configure Security - Set Optim Object Security Option
Optim
The Configuration program can Enable or Disable the Optim Object Security Feature for the current Optim Directory. Security can only be enabled or disabled by the Security Administrator. Select an option to enable or disable the Optim Object Security feature. Click <Proceed> to perform the action or <Skip> to bypass this step.
Optim Directory:
DIRECTORY
Security Feature:
Optim Object Security
Security State:
Disabled
Security Administrator for this Optim Directory
Domain\User Name:
NA\optusr3
Security Options for this Optim Directory
Enable
Disable
Secure Selected Objects When Saved
Edit Optim Object Template ACL...
Previous
Proceed
Skip
Cancel
Ready
Oracle-QOR922K

Optim Directory displays the directory name, and **Security Feature** indicates ***Optim*** Object Security is the option you can enable or disable. **Security State** indicates that security for the option is Enabled or Disabled. **Security Administrator for this Optim Directory** displays the Security Administrator.

Configuring Object Security

Use the **Set Optim Object Security Option** dialog to configure Object Security by doing the following:

- Enabling or disabling Object Security.

- Indicating whether selected objects are automatically assigned an ACL when saved.
- Defining the ***Optim*** Object Template ACL.

To enable or disable ***Optim*** Object Security, select **Enable** or **Disable**.

After configuring Object Security, click **Proceed**. If the Security Administrator is not signed on to the workstation, the **Specify Domain Connection Information** dialog is displayed and the password for the Security Administrator must be entered.

Automatically Assigning an ACL

Use the **Secure Selected Objects When Saved** option to automatically assign an ACL to an object when it is saved. The ACL is modeled after the ***Optim*** Object Template ACL. For more information about using the ***Optim*** Object Template ACL, see **Optim Object Template ACL**.

Note: **Secure Selected Objects When Saved** is available only when **Enable** is selected.

To automatically assign an ACL to an object, select **Secure Selected Objects When Saved**. When **Secure Selected Objects When Saved** is selected, the browse button is available. Click the browse button to open the **Select Optim Object Types** dialog, which allows you to select the types of ***Optim*** objects that are automatically assigned an ACL when they are saved.

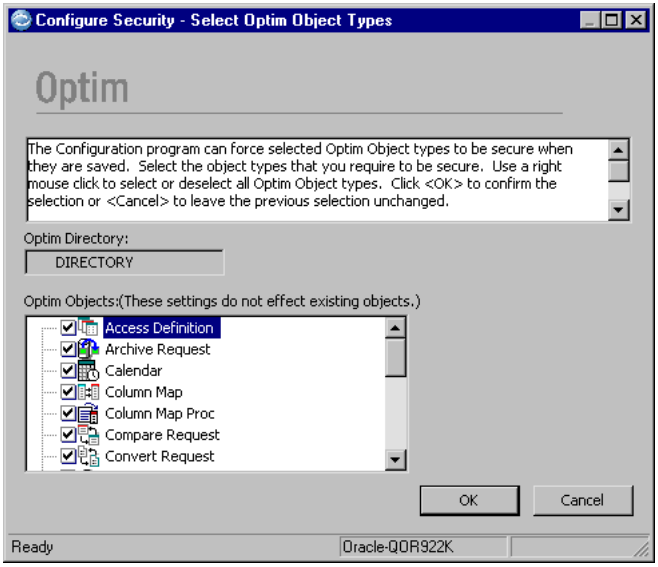
To secure objects with an ACL when saved:

1. In **Security Options for this Optim Directory**, select **Enabled**.
2. Select **Secure Selected Objects When Saved**.
3. Click the browse button to open the **Select Optim Object Types** dialog.
4. In the **Optim Objects List**, select the check box for each object type you want to automatically assign an ACL when saved.
5. Click **OK** to return to the **Set Optim Object Security Option** dialog.

Note: If **Secure Selected Objects When Saved** is selected, objects are automatically assigned an ACL when Object Security is either enabled or disabled.

Select Optim Object Types

Use the **Select Optim Object Types** dialog to select object types that are assigned an ACL when saved. Use the check boxes in the **Optim Objects** list to select the object types. To exclude an object type, clear the corresponding check box.


Configure Security - Select Optim Object Types
Optim
The Configuration program can force selected Optim Object types to be secure when they are saved. Select the object types that you require to be secure. Use a right mouse click to select or deselect all Optim Object types. Click <OK> to confirm the selection or <Cancel> to leave the previous selection unchanged.
Optim Directory:
DIRECTORY
Optim Objects:(These settings do not effect existing objects.)
Access Definition
Archive Request
Calendar
Column Map
Column Map Proc
Compare Request
Convert Request
OK
Cancel
Ready
Oracle-QOR922K

The following shortcut menu commands are available:

Select All	Select all objects in the list.
Deselect All	Clear all selections in the list.
Invert Selection	Reverse selected and unselected object types.

Optim Object Template ACL

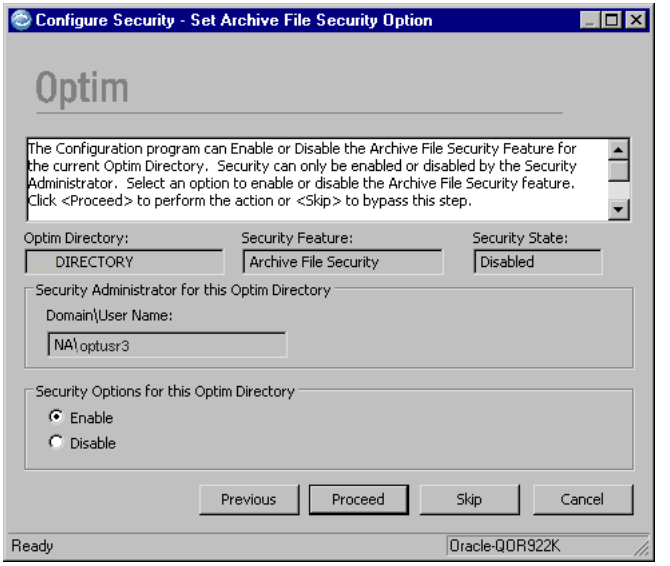
ACLs for ***Optim*** Objects are modeled after the Optim Object Template ACL. The Optim Object Template ACL does not secure any objects and can be edited by the Security Administrator only. The Security Administrator can open the **Access Control List Editor** and edit the Optim Object Template ACL from the **Configuration** program or the main window:

- From the **Configuration** program, click **Edit Optim Object Template ACL** from the **Set Optim Object Security Option** dialog.
- From the main window, click **Optim Object Template ACL** from the **Security** submenu on the **Options** menu.

For information about editing ACLs, see **D.2.1 Access Control List Editor** on page 471.

7.4.5 Set Archive File Security Option

The **Set Archive File Security Option** dialog allows the Security Administrator to enable or disable Archive File Security for the ***Optim*** Directory. Archive File Security controls access to tables and columns in Archive Files. For more information about Archive File Security, see **Archive File Security** on page 446.


Configure Security - Set Archive File Security Option
Optim
The Configuration program can Enable or Disable the Archive File Security Feature for the current Optim Directory. Security can only be enabled or disabled by the Security Administrator. Select an option to enable or disable the Archive File Security feature. Click <Proceed> to perform the action or <Skip> to bypass this step.
Optim Directory:
DIRECTORY
Security Feature:
Archive File Security
Security State:
Disabled
Security Administrator for this Optim Directory
Domain\User Name:
NA\optusr3
Security Options for this Optim Directory
Enable
Disable
Previous
Proceed
Skip
Cancel
Ready
Oracle-QOR922K

Optim Directory displays the directory name, and **Security Feature** indicates Archive File Security is the option you can enable or disable. **Security State** indicates that security for the option is Enabled or Disabled. **Security Administrator for this Optim Directory** displays the Security Administrator.

To enable or disable Archive File Security, select **Enable** or **Disable** and click **Proceed**. If the Security Administrator is not signed on to the workstation, the **Specify Domain Connection Information** dialog is displayed and the password for the Security Administrator must be entered.

7.5 Enable/Disable this Machine as an Optim Server

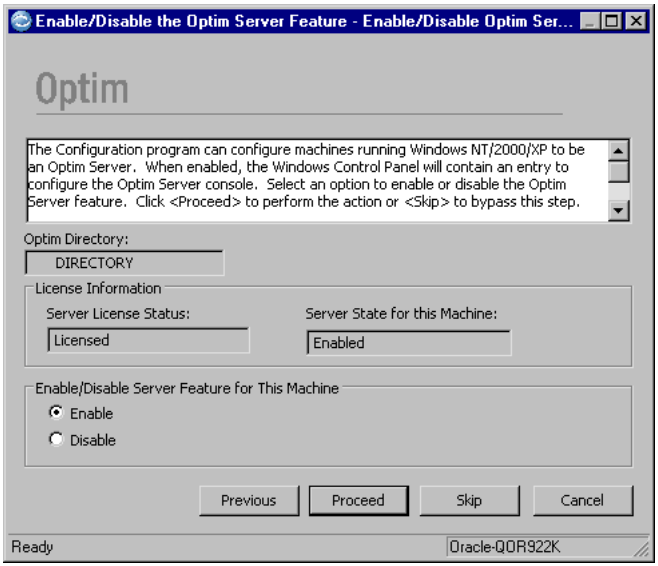
To change the status of a machine to or from that of a ***Server***, select **Enable/Disable this Machine as an Optim Server** from the **Tasks** menu.

Specify Optim Directory

The **Configuration** program displays the **Specify Optim Directory** dialog. The option to **Use Existing Optim Directory and Registry Entry** is selected. Specify the name of the ***Optim*** Directory you want to use. To select from a list, click the down arrow. To continue, click **Proceed**.

Enable/Disable Optim Server Feature

On the **Enable/Disable Optim Server Feature** dialog, specify whether to enable or disable the current machine as a ***Server***.


Enable/Disable the Optim Server Feature - Enable/Disable Optim Ser...
Optim
The Configuration program can configure machines running Windows NT/2000/XP to be an Optim Server. When enabled, the Windows Control Panel will contain an entry to configure the Optim Server console. Select an option to enable or disable the Optim Server feature. Click <Proceed> to perform the action or <Skip> to bypass this step.
Optim Directory:
DIRECTORY
License Information
Server License Status:
Licensed
Server State for this Machine:
Enabled
Enable/Disable Server Feature for This Machine
Enable
Disable
Previous
Proceed
Skip
Cancel
Ready
Oracle-QOR922K

If the site is not licensed for the ***Server***, **Enable** is not available. Refer to **Chapter 6. Configure the Optim Server** for configuration information.

7.6 Enable/Disable the ODBC Interface for this Machine

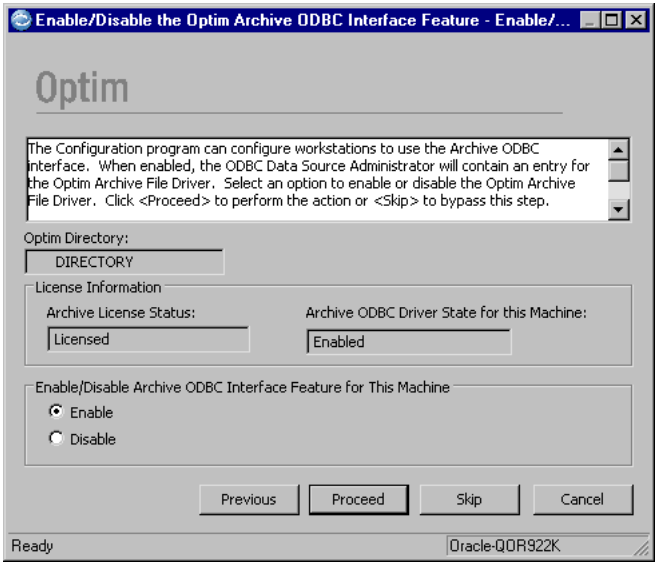
To enable or disable the ODBC interface capability of a machine, select **Enable/Disable the ODBC Interface for this Machine** from the **Tasks** menu.

Specify Optim Directory

The **Configuration** program displays the **Specify Optim Directory** dialog. The **Use Existing Optim Directory and Registry Entry** option is selected. Specify the name of the ***Optim*** Directory you want to use. Click the down arrow to select from a list. Click **Proceed** to continue.

Enable/Disable the Archive ODBC Interface Feature

On the **Enable/Disable the Archive ODBC Interface Feature** dialog, specify whether to enable or disable the ODBC driver.


Enable/Disable the Optim Archive ODBC Interface Feature - Enable/...
Optim
The Configuration program can configure workstations to use the Archive ODBC interface. When enabled, the ODBC Data Source Administrator will contain an entry for the Optim Archive File Driver. Select an option to enable or disable the Optim Archive File Driver. Click <Proceed> to perform the action or <Skip> to bypass this step.
Optim Directory:
DIRECTORY
License Information
Archive License Status:
Licensed
Archive ODBC Driver State for this Machine:
Enabled
Enable/Disable Archive ODBC Interface Feature for This Machine
Enable
Disable
Previous
Proceed
Skip
Cancel
Ready
Oracle-QOR922K

If the site is not licensed for ***Archive***, **Enable** is not available.

7.7 Apply Maintenance for Optim Directory Access

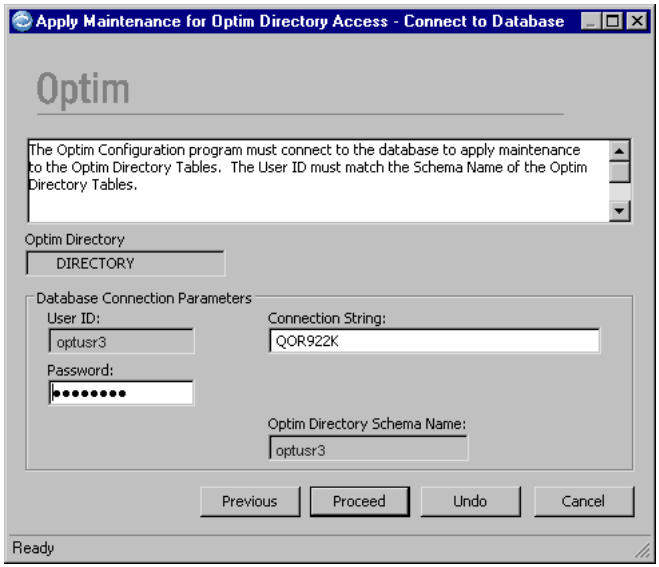
At times, it may be necessary to refresh or update the packages, plans, or procedures needed to access the ***Optim*** Directory tables. Generally, you apply maintenance for ***Optim*** Directory access when installing a new version of ***Optim***. However, if you drop the ***Optim*** Directory tables for some reason, you must apply maintenance to recreate the necessary packages, plans, or procedures. To refresh or update the packages, plans, or procedures for the ***Optim*** Directory tables, select **Apply Maintenance for Optim Directory Access** from the **Tasks** menu.

Specify *Optim* Directory

The first step in applying maintenance for ***Optim*** Directory access is to provide the name of the ***Optim*** Directory. The **Configuration** program prompts for this information by presenting the **Specify Optim Directory** dialog (see page 79). You must select **Use Existing Optim Directory and Registry Entry**, select an ***Optim*** Directory name, and click **Proceed** to open the next dialog.

Connect to Database

When applying maintenance for ***Optim*** Directory access, the **Configuration** program must connect to the database to create or refresh the packages, plans, or procedures. On the **Connect to Database** dialog, you must provide the **User ID**, **Password**, and **Connection String** that the workstation needs to connect to the ***Optim*** Directory.



On this dialog, when you apply maintenance for ***Optim*** Directory access, the User ID must match the identifier for ***Optim*** Directory tables.

Create/Drop Packages

Before creating or refreshing packages, plans, or procedures for the ***Optim*** Directory tables, the **Configuration** program displays the **Create/Drop Packages** or **Create/Drop Stored Procedures** dialog (see page 85), or the **Bind/Drop Plans** dialog (see page 87). You can choose to browse the DDL statements generated to create or refresh the packages, plans, or procedures. In addition, if the specified ***Optim*** Directory tables are not the ones you want to use, you can cancel the process.

Add Default Tables

After packages, plans, or procedures are created for the ***Optim*** Directory, the **Configuration** program prompts you to add default tables to the ***Optim*** Directory. If you select the check box, the **Configuration** program verifies that default Calendars and Currency tables are in the ***Optim*** Directory. If not found, these tables are loaded automatically.

Apply Maintenance to Another?

Before completing the task to **Apply Maintenance for Optim Directory Access**, the **Configuration** program prompts you to apply maintenance for access to another ***Optim*** Directory. If you select the check box, you can repeat the maintenance process. To end the task, clear the check box and click **Proceed**.

7.8 Apply Maintenance for DB Alias Access

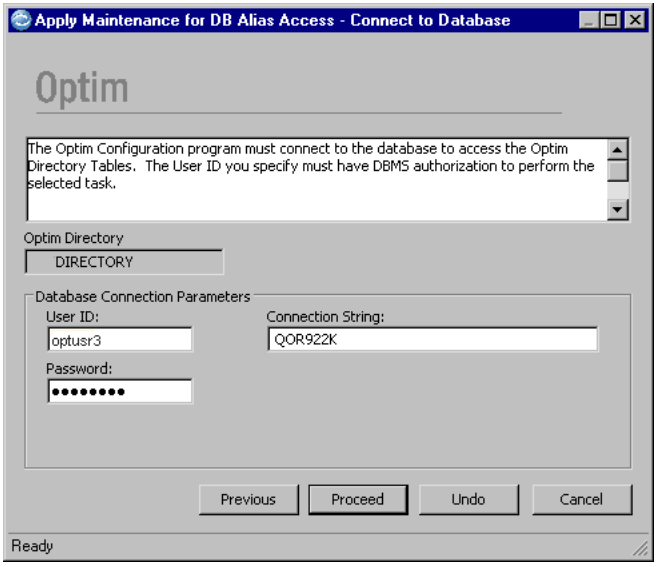
At times, it may be necessary to refresh or update the packages, plans, or procedures needed to access database tables. Generally, you apply maintenance for DB Alias access only when you are installing a new version of ***Optim*** or to recreate packages, plans, or procedures. To refresh or update the packages, plans, or procedures for database tables, select **Apply Maintenance for DB Alias Access** from the **Tasks** menu.

Specify Optim Directory

The first step in applying maintenance for DB Alias access is to **Specify an Optim Directory** (see page 185). You must select an ***Optim*** Directory name and click **Proceed** to open the next dialog.

Connect to Database

When applying maintenance for DB Alias access, the **Configuration** program must connect to the database to access ***Optim*** Directory Tables.

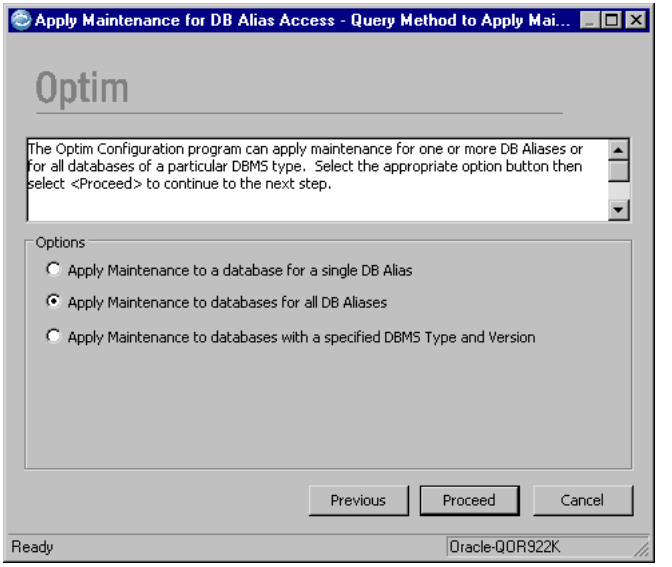


On the **Connect to Database** dialog, you must specify the **User ID**, **Password**, and **Connection String** that allows the workstation to connect to the database to access ***Optim*** Directory tables.

Note: The **User ID** you specify must have the authorization to perform this maintenance task.

7.8.1 Query Method to Apply Maintenance?

After you specify the ***Optim*** Directory and connect to the database, the **Configuration** program displays the **Query Method to Apply Maintenance?** dialog. Select the level of maintenance to apply.


Apply Maintenance for DB Alias Access - Query Method to Apply Mai...
Optim
The Optim Configuration program can apply maintenance for one or more DB Aliases or for all databases of a particular DBMS type. Select the appropriate option button then select <Proceed> to continue to the next step.
Options
Apply Maintenance to a database for a single DB Alias
Apply Maintenance to databases for all DB Aliases
Apply Maintenance to databases with a specified DBMS Type and Version
Previous
Proceed
Cancel
Ready
Oracle-QOR922K

To apply maintenance to create or refresh packages, plans, or procedures needed to access database tables, select one of the following options:

- **Apply Maintenance to a database for a single DB Alias** — Select this option to apply maintenance to a database referenced by a specific DB Alias in the selected ***Optim*** Directory.
- **Apply Maintenance to databases for all DB Aliases** — Select this option to apply maintenance to databases referenced by each DB Alias in the selected ***Optim*** Directory.
- **Apply Maintenance to databases with a specified DBMS Type and Version** — Select this option to apply maintenance to each database of a particular DBMS Type and version in the selected ***Optim*** Directory.

7.8.2 Apply Maintenance for a Single DB Alias

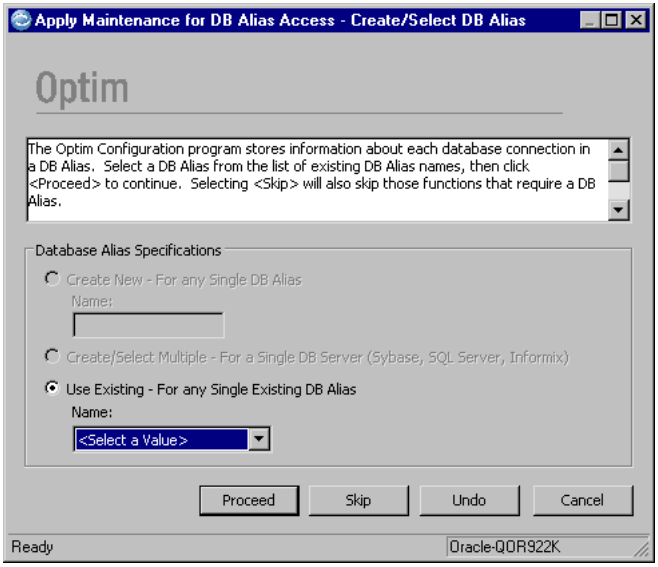
If you select the option on the **Query Method to Apply Maintenance?** dialog to apply maintenance for a single DB Alias, the task includes the following:

1. Create/Select the DB Alias.
2. Connect to the Database.
3. Drop old Packages, Plans, or Procedures.
4. Create/Refresh Packages, Plans, or Procedures.

After maintenance is applied, the task is complete, or you can choose to apply maintenance for another DB Alias.

Create/Select DB Alias

When you select **Apply Maintenance to a database for a single DB Alias**, the **Configuration** program opens the **Create/Select DB Alias** dialog allowing you to select the DB Alias for maintenance.


Apply Maintenance for DB Alias Access - Create/Select DB Alias
Optim
The Optim Configuration program stores information about each database connection in a DB Alias. Select a DB Alias from the list of existing DB Alias names, then click <Proceed> to continue. Selecting <Skip> will also skip those functions that require a DB Alias.
Database Alias Specifications
Create New - For any Single DB Alias
Name:
Create/Select Multiple - For a Single DB Server (Sybase, SQL Server, Informix)
Use Existing - For any Single Existing DB Alias
Name:
<Select a Value>
Proceed
Skip
Undo
Cancel
Ready
Oracle-QOR922K

The only available option is to use an existing DB Alias. Specify the name of the DB Alias you want to use. To select from a list, click the down arrow. Click **Proceed** to open the **Connect to Database** dialog.

Connect to Database

The **Configuration** program must connect to the database to apply maintenance to the Data Dictionary, Catalog Tables, or System Tables, depending on the DBMS you are using. When the **Connect to**

Database dialog opens, the **User ID**, **Password**, **Connection String**, and **DB Name** are populated with previously entered values.

The User ID you specify must have DBMS authorization to create or refresh database packages, plans, or procedures. You can modify these values, as needed, and click **Proceed** to continue.

Drop Old Packages

The **Configuration** program displays the **Drop Old Packages (Plans, or Procedures)** dialog. If you select this option and click **Proceed**, you can drop old packages, plans, or procedures before creating new ones. If you do not select this option, you can create/refresh the appropriate packages, plans, or procedures. The following guidelines apply:

- If you share stored procedures with other users, then any one authorized user can drop old packages (plans or procedures) for all users.
- If your qualifier is not used by anyone else, you can safely drop the old packages (plans or procedures) without affecting other users.

Note: If the same qualifier applies to multiple users, or if you regularly run different builds of ***Optim***, then you may not want to drop the old packages (plans or procedures).

Create/Drop Packages

The **Configuration** program displays the **Create/Drop Packages** dialog (see page 85), the **Bind/Drop Plans** dialog, or the **Create/Drop Stored Procedures** dialog, as appropriate for the DBMS you are using. This dialog allows you to **Create/Refresh** the:

- Packages to access the Data Dictionary in Oracle.
- Plans to access Catalog Tables in DB2.
- Procedures to access System Tables in Sybase ASE or SQL Server.
- Procedures to access Catalog Tables in Informix.

Apply Maintenance to Another?

After you apply maintenance for a single DB Alias, the **Configuration** program opens the **Apply Maintenance to Another DB Alias?** dialog and prompts you to apply maintenance for another DB Alias:

- To apply maintenance for another DB Alias, select the check box and click **Proceed** to open the **Create/Select DB Alias** dialog.
- To end the task, clear the check box and click **Proceed** to open the **Complete** dialog.

7.8.3 Apply Maintenance for All DB Aliases

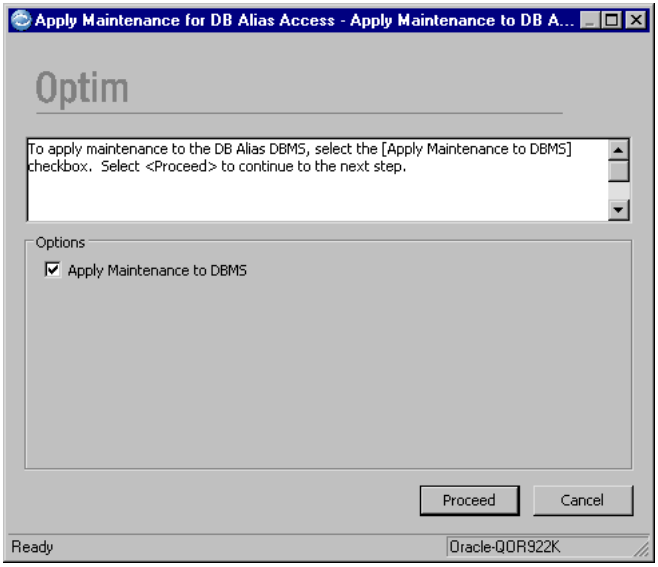
If you select the option on the **Query Method to Apply Maintenance** dialog, to apply maintenance for all DB Aliases, the task includes the following:

1. Choose to apply maintenance to the first or another DB Alias.
2. Connect to the Database.
3. Drop old Packages, Plans, or Procedures.
4. Create/Refresh Packages, Plans, or Procedures.

After maintenance is applied, you can choose to apply maintenance for the next in a series of DB Aliases, or the maintenance task is complete.

Apply Maintenance to DB Alias?

When you select **Apply Maintenance to databases for all DB Aliases**, the **Configuration** program prompts you to confirm maintenance for each DB Alias in the selected ***Optim*** Directory one at a time.


Apply Maintenance for DB Alias Access - Apply Maintenance to DB A...
Optim
To apply maintenance to the DB Alias DBMS, select the [Apply Maintenance to DBMS] checkbox. Select <Proceed> to continue to the next step.
Options
Apply Maintenance to DBMS
Proceed
Cancel
Ready
Oracle-QOR922K

On the **Apply Maintenance to DB Alias?** dialog, you can do the following:

- To apply maintenance for the named DB Alias, select the check box and click **Proceed** to open the **Connect to Database** dialog.

- To bypass maintenance for the named DB Alias, clear the check box and click **Proceed**. The **Configuration** program prompts you to apply maintenance for the next DB Alias.

Note: The steps to connect to the database and create/drop packages, plans or procedures are the same as those described to apply maintenance for a single DB Alias.

Apply Maintenance to Another?

After you apply maintenance for a DB Alias, the **Configuration** program opens the **Apply Maintenance to Another DB Alias?** dialog and prompts you to apply maintenance for another DB Alias.

- To apply maintenance for another DB Alias, select the check box and click **Proceed** to open the **Connect to Database** dialog.
- To end the task, clear the check box and click **Proceed** on each subsequent dialog until the **Complete** dialog displays.

7.8.4 Apply Maintenance for Specific DBMS

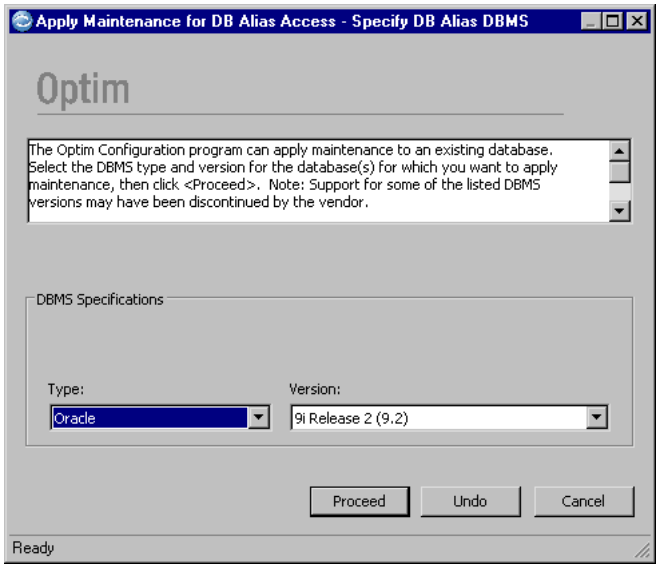
If you select the option on the **Query Method to Apply Maintenance** dialog, to apply maintenance for a specific DBMS, the task includes the following:

1. Specify the DB Alias DBMS (Type and Version).
2. Choose to apply maintenance for the first or another DB Alias.
3. Connect to the Database.
4. Drop old Packages, Plans, or Procedures.
5. Create/Refresh Packages, Plans, or Procedures.

After maintenance is applied, you can choose to apply maintenance to databases in a different DBMS, or the maintenance task is complete.

Specify DB Alias DBMS

When you select **Apply Maintenance to databases with a specified DBMS Type and Version**, the **Configuration** program opens the **Specify DB Alias DBMS** dialog.

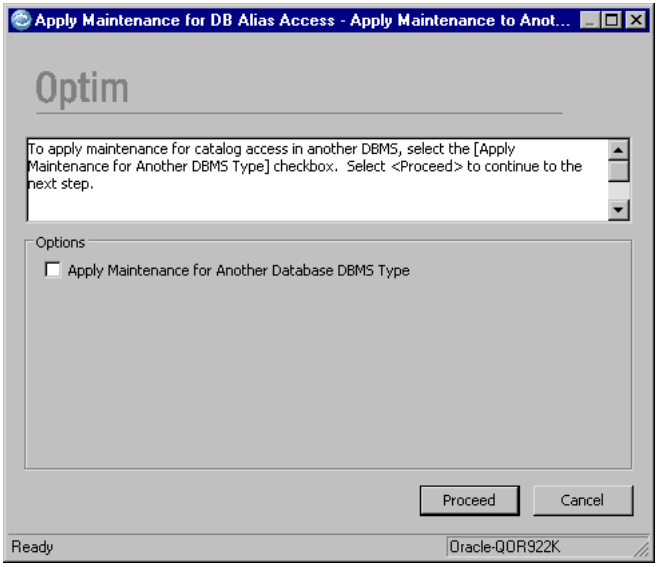

Apply Maintenance for DB Alias Access - Specify DB Alias DBMS
Optim
The Optim Configuration program can apply maintenance to an existing database. Select the DBMS type and version for the database(s) for which you want to apply maintenance, then click <Proceed>. Note: Support for some of the listed DBMS versions may have been discontinued by the vendor.
DBMS Specifications
Type:
Oracle
Version:
9i Release 2 (9.2)
Proceed
Undo
Cancel
Ready

Specify the DBMS **Type** and **Version**, and click **Proceed** to open the **Apply Maintenance to DB Alias?** dialog. To continue, select the DB Alias, connect to the database, and create/drop packages, plans, or procedures.

Note: The steps are the same as those previously described to apply maintenance for all DB Aliases.

Apply Maintenance to Another DBMS Type?

After you apply maintenance to the database in the selected DBMS, the **Configuration** program opens the **Apply Maintenance to Another DBMS Type?** dialog, and prompts you to confirm maintenance for a different database DBMS.


Apply Maintenance for DB Alias Access - Apply Maintenance to Anot...
Optim
To apply maintenance for catalog access in another DBMS, select the [Apply Maintenance for Another DBMS Type] checkbox. Select <Proceed> to continue to the next step.
Options
Apply Maintenance for Another Database DBMS Type
Proceed
Cancel
Ready
Oracle-QOR922K

On this dialog, you can do the following:

- To apply maintenance for another DBMS, select the check box and click **Proceed** to open the **Specify DB Alias DBMS** dialog.
- To end the task, clear the check box and click **Proceed** on each subsequent dialog until the **Complete** dialog displays.

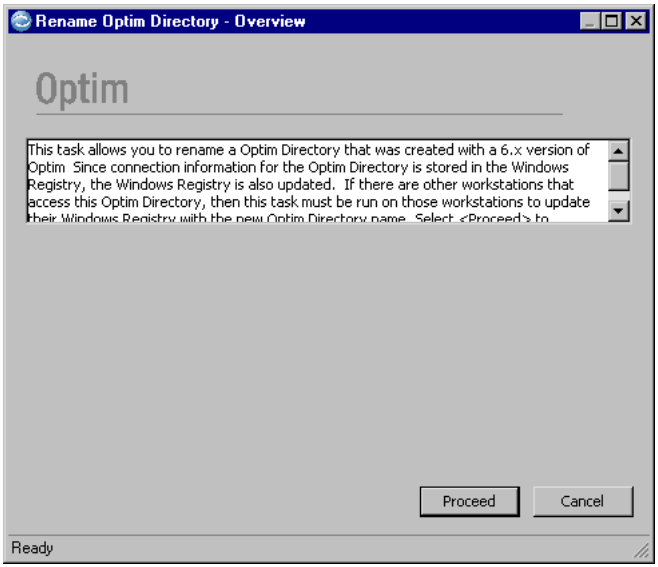
7.9 Rename an Optim Directory

At times, you may rename an ***Optim*** Directory. For example, upgrading from version 5.x to version 6.x requires that you create a new Directory and convert ***Optim*** objects created before the upgrade, as described in **Appendix G. Converting PST and Optim Directory Objects**. Once the new Directory is created and the old Directory is deleted, you can rename the new Directory to use it in place of the old Directory. To delete a Directory, see **7.17 Drop DB Alias or Optim Tables**.

To rename the new Directory, you must replace the name in the Directory itself and in the Windows registry on each workstation that accesses the Directory. Select **Rename an Optim Directory** from the **Tasks** menu to change the name in the ***Optim*** Directory and workstation registry or, once the ***Optim*** Directory is changed, to re-name a registry entry or register the re-named Directory on a workstation.

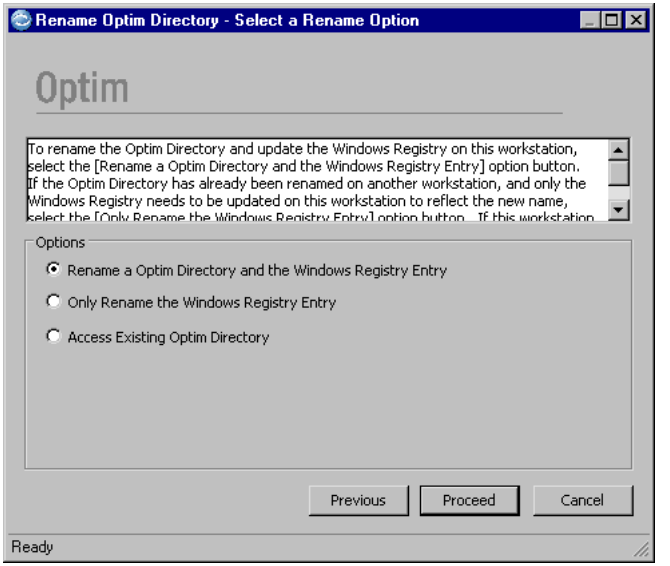
Overview

When you select **Rename an Optim Directory** from the **Tasks** menu, the **Overview** dialog provides an overview of the task. To continue, click **Proceed**.


Rename Optim Directory - Overview
Optim
This task allows you to rename a Optim Directory that was created with a 6.x version of Optim. Since connection information for the Optim Directory is stored in the Windows Registry, the Windows Registry is also updated. If there are other workstations that access this Optim Directory, then this task must be run on those workstations to update
Proceed
Cancel
Ready

Select a Rename Option

The first step in renaming an ***Optim*** Directory is to **Select a Rename Option**.

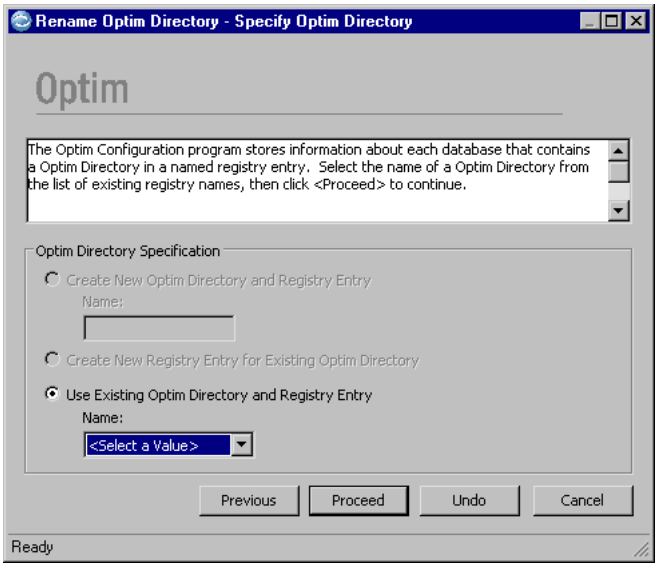

Rename Optim Directory - Select a Rename Option
Optim
To rename the Optim Directory and update the Windows Registry on this workstation, select the [Rename a Optim Directory and the Windows Registry Entry] option button. If the Optim Directory has already been renamed on another workstation, and only the Windows Registry needs to be updated on this workstation to reflect the new name,
Options
Rename a Optim Directory and the Windows Registry Entry
Only Rename the Windows Registry Entry
Access Existing Optim Directory
Previous
Proceed
Cancel
Ready

- **Rename a Optim Directory and the Windows Registry Entry** — Select this option to rename an ***Optim*** Directory in the Directory tables and the Windows registry on the workstation. To rename a Directory, this option needs to be performed only once.
- **Only Rename the Windows Registry Entry** — Select this option to rename the ***Optim*** Directory in the Windows registry on the workstation. Use this option on each workstation that uses a renamed Directory.
- **Access Existing Optim Directory** — Select this option to register an ***Optim*** Directory in the Windows registry on the workstation. This option allows you to perform the Access Existing Optim Directory task (see page 191).

7.9.1 Rename an *Optim* Directory and the Windows Registry Entry

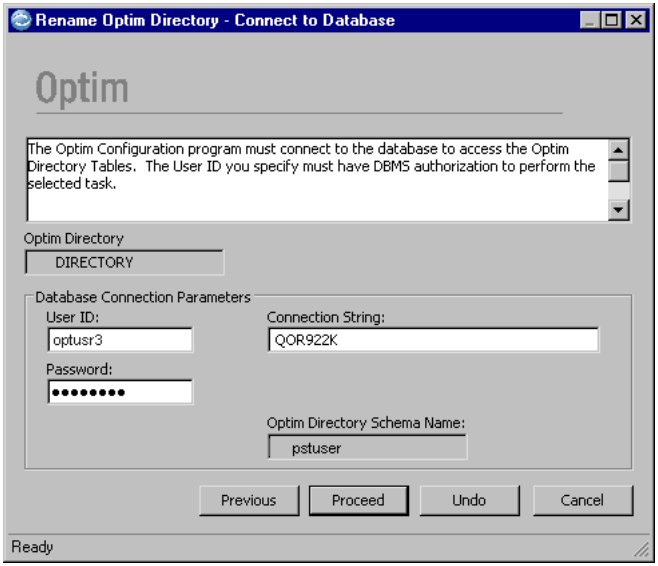
Specify *Optim* Directory

After selecting the option to rename an ***Optim*** Directory, the **Specify Optim Directory** dialog is displayed. The option to **Use Existing Optim Directory and Registry Entry** is selected. Specify the **Name** of the Directory you want to rename. To select from a list, click the down arrow.


Rename Optim Directory - Specify Optim Directory
Optim
The Optim Configuration program stores information about each database that contains a Optim Directory in a named registry entry. Select the name of a Optim Directory from the list of existing registry names, then click <Proceed> to continue.
Optim Directory Specification
Create New Optim Directory and Registry Entry
Name:
Create New Registry Entry for Existing Optim Directory
Use Existing Optim Directory and Registry Entry
Name:
<Select a Value>
Previous
Proceed
Undo
Cancel
Ready

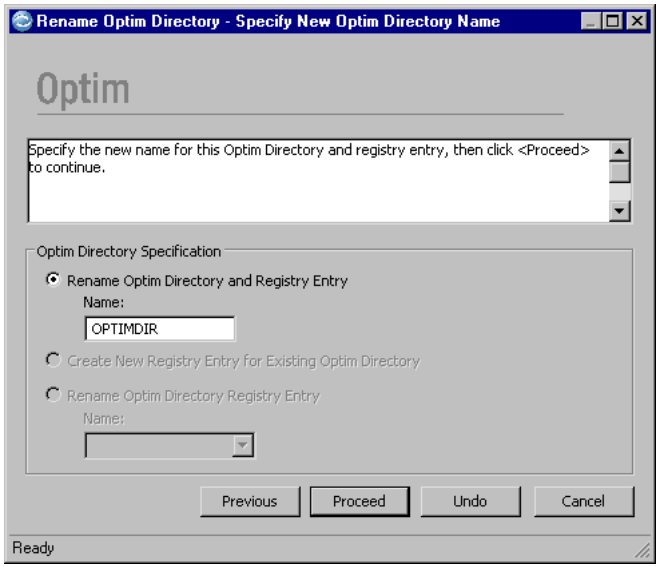
Connect to Database

When renaming an ***Optim*** Directory, the **Configuration** program must connect to the database and verify the user has authorization to perform the task. On the **Connect to Database** dialog, you must specify the **User ID**, **Password**, and **Connection String** that the workstation needs to connect to the Directory.



Specify New Optim Directory Name

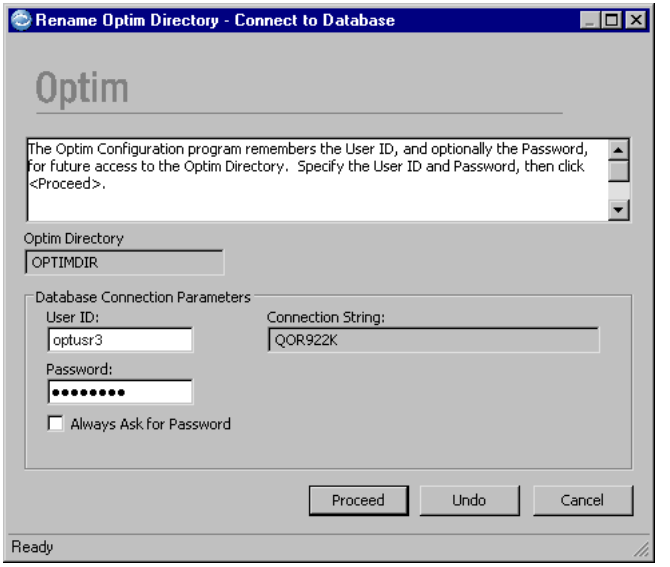
After connecting to the database, the **Specify New Optim Directory Name** dialog is displayed, allowing you to rename the ***Optim*** Directory and the registry entry.



The option to **Rename Optim Directory and Registry Entry** is selected. Specify the new **Name** for the ***Optim*** Directory. A Directory name can be from 1 to 12 characters and have no embedded blanks. The new Directory name cannot match an existing Directory name.

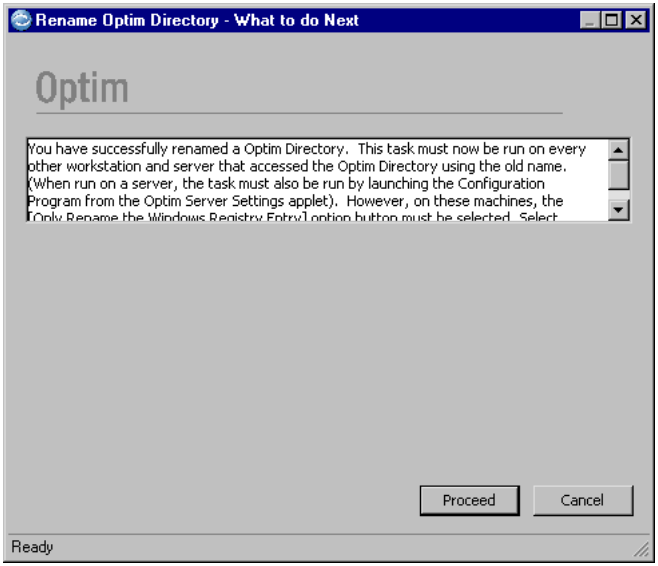
Connect to Database

After an ***Optim*** Directory is renamed, the **Configuration** program updates connection information in the registry entry. For subsequent access to the Directory from this workstation, use the **Connect to Database** dialog to specify a **User ID** and **Password** (see page 93). Click **Proceed** to display the **Complete** dialog and complete the process.



What to do Next

After connection information is updated in the registry, the **What to do Next** dialog instructs you to use the **Only Rename the Windows Registry Entry** option to update the registry for each workstation that accesses the ***Optim*** Directory. Click **Proceed** to display the **Complete** dialog and complete the process.

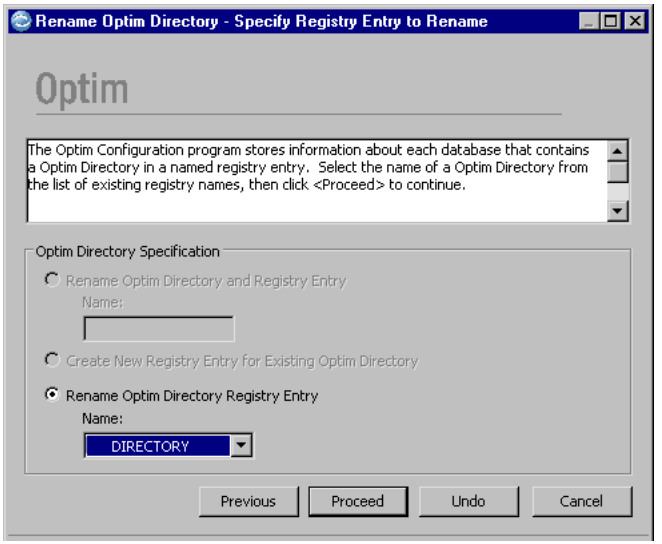

Rename Optim Directory - What to do Next
Optim
You have successfully renamed a Optim Directory. This task must now be run on every other workstation and server that accessed the Optim Directory using the old name. (When run on a server, the task must also be run by launching the Configuration Program from the Optim Server Settings applet). However, on these machines, the
Proceed
Cancel
Ready

7.9.2 Only Rename the Windows Registry Entry

Specify Registry Entry to Rename

After selecting the option to rename a registry entry, the **Specify Registry Entry to Rename** dialog is displayed. The option to **Rename Optim Directory Registry Entry** is selected. Specify the **Name** of the

Optim Directory you want to rename in the registry. To select from a list, click the down arrow.

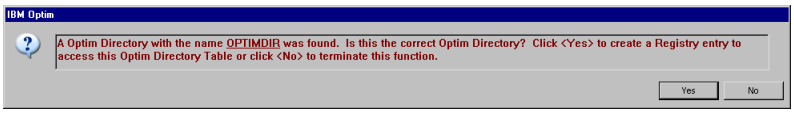

Rename Optim Directory - Specify Registry Entry to Rename
Optim
The Optim Configuration program stores information about each database that contains a Optim Directory in a named registry entry. Select the name of a Optim Directory from the list of existing registry names, then click <Proceed> to continue.
Optim Directory Specification
Rename Optim Directory and Registry Entry
Name:
Create New Registry Entry for Existing Optim Directory
Rename Optim Directory Registry Entry
Name:
DIRECTORY
Previous
Proceed
Undo
Cancel

Connect to Database

When renaming an ***Optim*** Directory registry entry, the **Configuration** program must connect to the database and verify the user has authorization to perform the task. On the **Connect to Database** dialog, you must specify the **User ID**, **Password**, and **Connection String** that the workstation needs to connect to the Directory.

Confirm the Optim Directory Name

After connecting to the database, a pop-up dialog displays the new ***Optim*** Directory name. Click **Yes** to confirm the new name and rename the registry entry. Click **No** to terminate the process.


IBM Optim
A Optim Directory with the name OPTIMDIR was found. Is this the correct Optim Directory? Click <Yes> to create a Registry entry to access this Optim Directory Table or click <No> to terminate this function.
Yes
No

Connect to Database

After an ***Optim*** Directory registry entry is renamed, the **Configuration** program updates connection information in the registry entry. For subsequent access to the Directory from this workstation, use the **Connect to Database** dialog to specify a **User ID** and **Password** (see page 93). Click **Proceed** to display the **Complete** dialog and complete the process.

7.10 Update DBMS Version for an Optim Directory

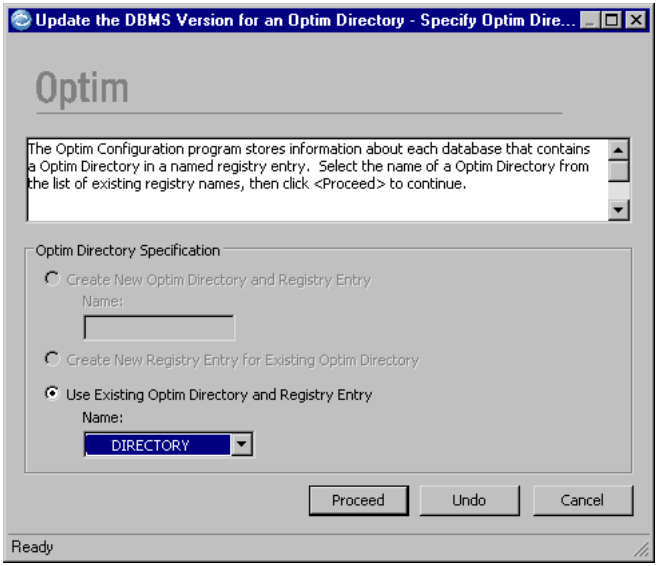
When you select **Update the DBMS Version for an Optim Directory** from the **Tasks** menu, the first dialog cautions that you should select this task *only* when the ***Optim*** Directory resides in a database that has been upgraded to a new version. This task prompts you to:

1. Select the ***Optim*** Directory to update and select the new DBMS version.
2. Drop the old packages, plans, or procedures and create new ones for the ***Optim*** Directory.
3. Update the database signature for the ***Optim*** Directory**.**

When the process completes, the database signature is updated automatically.

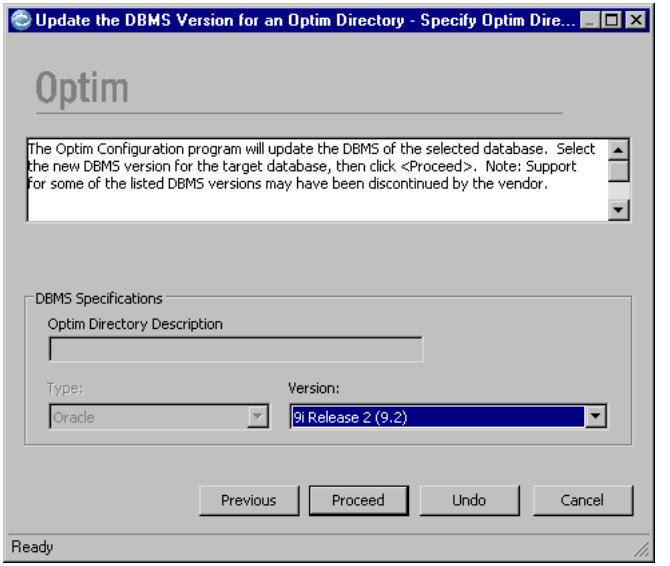
Specify Optim Directory

The first step in updating the DBMS version for an ***Optim*** Directory is to specify the name of the Directory. Click the down arrow to select from a list and click **Proceed**.


Update the DBMS Version for an Optim Directory - Specify Optim Dire...
Optim
The Optim Configuration program stores information about each database that contains a Optim Directory in a named registry entry. Select the name of a Optim Directory from the list of existing registry names, then click <Proceed> to continue.
Optim Directory Specification
Create New Optim Directory and Registry Entry
Name:
Create New Registry Entry for Existing Optim Directory
Use Existing Optim Directory and Registry Entry
Name:
DIRECTORY
Proceed
Undo
Cancel
Ready

Specify Optim Directory DBMS

You must specify the version of the DBMS you want to use to update the ***Optim*** Directory.


Update the DBMS Version for an Optim Directory - Specify Optim Dire...
Optim
The Optim Configuration program will update the DBMS of the selected database. Select the new DBMS version for the target database, then click <Proceed>. Note: Support for some of the listed DBMS versions may have been discontinued by the vendor.
DBMS Specifications
Optim Directory Description
Type:
Oracle
Version:
9i Release 2 (9.2)
Previous
Proceed
Undo
Cancel
Ready

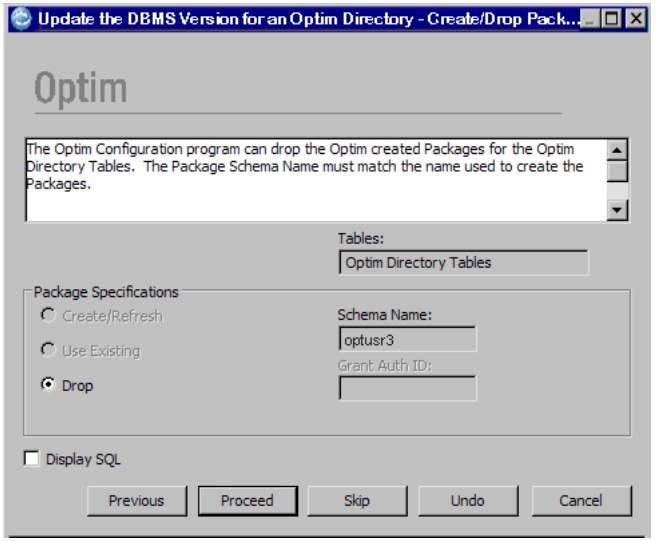
Click the down arrow to select a version. The version you select must be different from the current version. If not, an error message displays. Click **Proceed** to connect to the database.

Connect to Database

When you update information for the ***Optim*** Directory, the **Configuration** program must connect to the database to access the ***Optim*** Directory Tables. On the **Connect to Database** dialog (see page 205), you must specify the **User ID**, **Password**, and **Connection String** that allows the workstation to connect to the database. If the connection is successful, the next step is to drop the old packages, plans, or procedures and create new ones for the updated DBMS.

Create/Drop Packages

The **Configuration** program displays the **Create/Drop Packages** dialog, the **Create/Drop Stored Procedures** dialog, or the **Bind/Drop Plans** dialog, as appropriate for the DBMS you are using.



The **Drop** option is selected when this dialog opens. You can select the **Display SQL** check box to browse the DDL statements generated for the drop process. To continue, click **Proceed**.

Note: The **Configuration** program attempts to drop all old packages, plans, and procedures for the specified DBMS version, even if they were never installed.

After the **Drop** process completes, this dialog redisplays with the **Create/Refresh** option selected automatically. Click **Proceed** to create packages, plans, or procedures to update the DBMS for the ***Optim*** Directory.

When the process completes, the database signature is updated automatically and the **Complete** dialog displays.

7.11 Update DBMS Version for a DB Alias

When you select **Update DBMS Version for a DB Alias** from the **Tasks** menu, the first dialog cautions that you should select this task *only* when a DB Alias refers to a database that has been upgraded to a new version. This task prompts you to:

1. Select the ***Optim*** Directory containing the DB Alias.
2. Select the DB Alias and select the new DBMS version.
3. Drop the old packages, plans, or procedures and create new ones for the ***Optim*** Directory.

When this process completes, the database signature is updated automatically.

7.11.1 Update DBMS for a Single DB Alias

You can update the DBMS version for a single DB alias; however, if you are using Sybase ASE, SQL Server, or Informix and you have multiple databases on one server, the **Configuration** program automatically directs you to the appropriate dialogs. The initial steps are the same whether you are updating the DBMS version for one DB Alias or multiple DB Aliases.

Specify Optim Directory

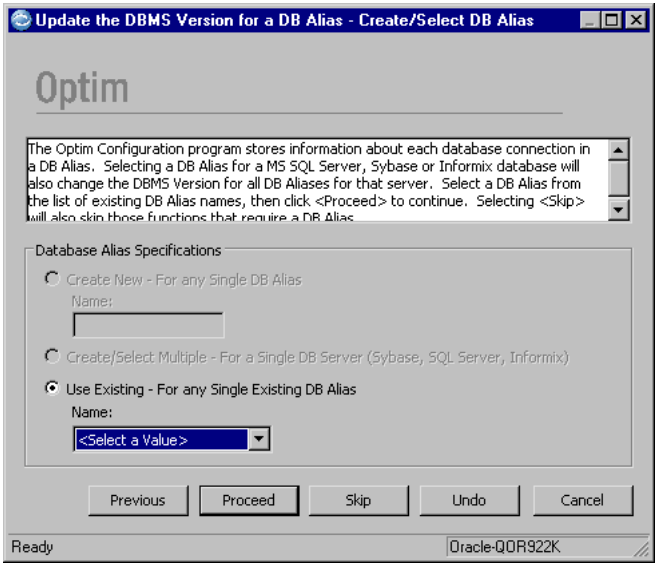
The first step in updating the DBMS version for a DB Alias is to specify the name of the ***Optim*** Directory associated with that DB Alias. Click the down arrow to select an ***Optim*** Directory from a list and click **Proceed** to connect to the database.

Connect to Database

The **Configuration** program must connect to the database to access the ***Optim*** Directory Tables. On the **Connect to Database** dialog (see page 205), you must specify the **User ID**, **Password**, and **Connection String** that allows the workstation to connect to the database. If the connection is successful, you can create or select a DB Alias.

Create/Select DB Alias

The next step is to select the DB Alias to update the corresponding DBMS version.

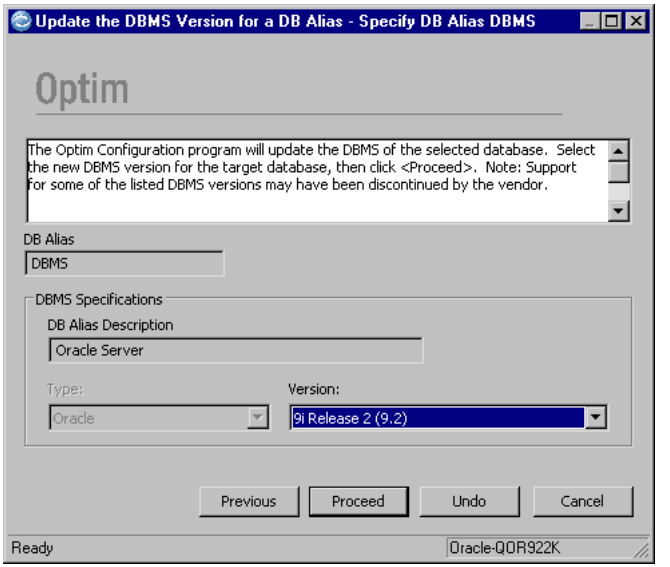

Update the DBMS Version for a DB Alias - Create/Select DB Alias
Optim
The Optim Configuration program stores information about each database connection in a DB Alias. Selecting a DB Alias for a MS SQL Server, Sybase or Informix database will also change the DBMS Version for all DB Aliases for that server. Select a DB Alias from the list of existing DB Alias names, then click <Proceed> to continue. Selecting <Skip>
Database Alias Specifications
Create New - For any Single DB Alias
Name:
Create/Select Multiple - For a Single DB Server (Sybase, SQL Server, Informix)
Use Existing - For any Single Existing DB Alias
Name:
<Select a Value>
Previous
Proceed
Skip
Undo
Cancel
Ready
Oracle-QOR922K

Click the down arrow to select a DB Alias from the list of existing DB Alias names, then click **Proceed** to continue.

Note: If you are using SQL Server, Sybase ASE, or Informix, and have several databases on one server, the **Configuration** program automatically selects every DB Alias that resides on the same server.

Specify DB Alias DBMS

You must specify the DBMS version to use for the selected DB Alias.


Update the DBMS Version for a DB Alias - Specify DB Alias DBMS
Optim
The Optim Configuration program will update the DBMS of the selected database. Select the new DBMS version for the target database, then click <Proceed>. Note: Support for some of the listed DBMS versions may have been discontinued by the vendor.
DB Alias
DBMS
DBMS Specifications
DB Alias Description
Oracle Server
Type:
Oracle
Version:
9i Release 2 (9.2)
Previous
Proceed
Undo
Cancel
Ready
Oracle-QOR922K

Click the down arrow to select a version from the list. The version you select must be different from the current version. If not, an error message displays. To continue, click **Proceed**.

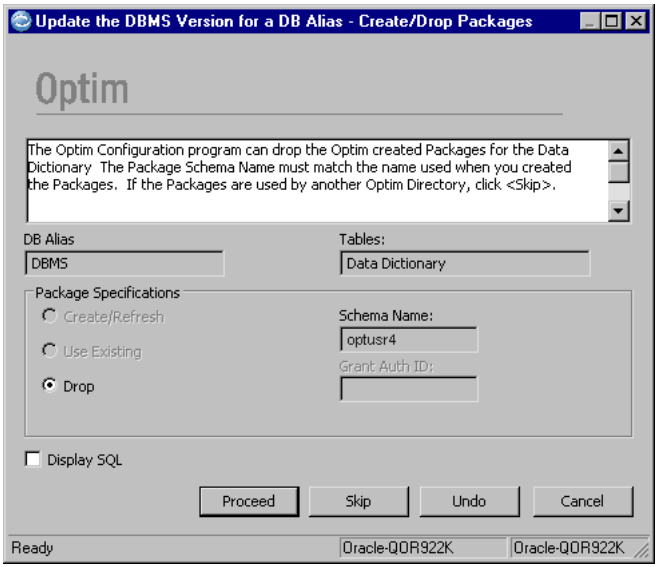
Connect to Database

If you are updating the DBMS version for only one DB Alias, the **Connect to Database** dialog opens. You specify the **User ID**, **Password**, and **Connection String** needed to connect to the selected database.

Note: If you are updating the DBMS version for Sybase ASE, SQL Server, or Informix, and you have several databases on one server, refer to **7.11.2 Update Multiple DB Aliases** for complete details.

Create/Drop Packages

The **Configuration** program displays the **Create/Drop Packages** dialog, the **Create/Drop Stored Procedures** dialog, or the **Bind/Drop Plans** dialog, as appropriate for the DBMS you are using.



The **Drop** option is selected when this dialog opens. You can select the **Display SQL** check box to browse the DDL statements generated for the process. To continue, click **OK**.

After the **Drop** process completes, this dialog redisplays with the **Create/Refresh** option selected automatically. Click **Proceed** to create the following:

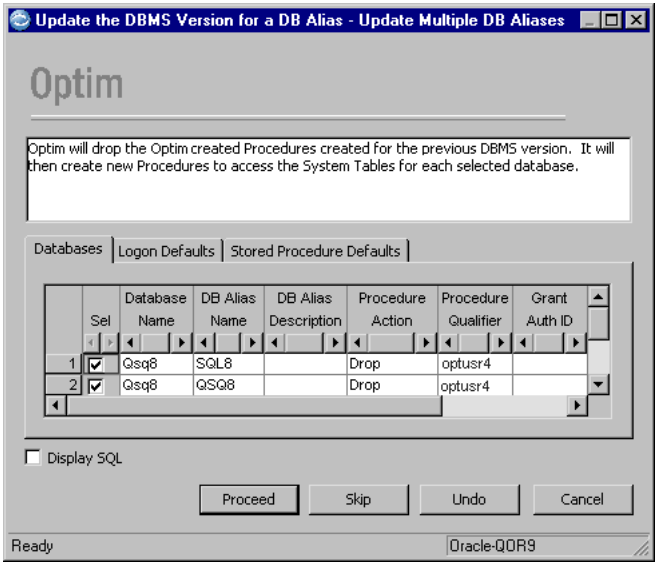
- Packages to access the Data Dictionary in Oracle.
- Plans to access Catalog Tables in DB2.
- Procedures to access System Tables in Sybase ASE or SQL Server.
- Procedures to access Catalog Tables in Informix.

When the process completes, the database signature is updated automatically and the **Complete** dialog displays.

7.11.2 Update Multiple DB Aliases

If you are updating the DBMS version for Sybase ASE, SQL Server, or Informix, you may have several databases on one server. The procedure to update the DBMS for multiple DB Aliases is similar to the procedure for updating the DBMS for a single DB Alias.

After you select the DB Alias and specify the new DBMS version, the **Configuration** program automatically displays the following dialog showing all the DB Aliases that reside on a particular server.



The **Update Multiple DB Aliases** dialog displays the following tabs:

Databases — Review a list of all databases that reside on the single server. Specify explicit information for each DB Alias you want to update.

Logon Defaults — Specify the default **User ID** and **Password** needed to create/refresh stored procedures while configuring the first or additional workstations. In some cases, this logon may have additional privileges than the Saved Logon Defaults.

Stored Procedure Defaults Specify the default procedure **Qualifier** and **Grant Auth ID** required to create/refresh stored procedures.

Note: The default values apply to all DB Aliases, unless otherwise specified on the **Databases** tab.

Databases Tab

Use the **Databases** tab to review a list of all databases that reside on the single server. You can also specify explicit details for the DB Aliases you want to update:

Sel Select a check box to update a DB Alias for a particular database. If you do not want to update a DB Alias, clear the check box. This grid column is locked in position, so you can scroll to the left or right and still see the selected databases.

Database Name Name assigned to the database when it was created.

DB Alias Description Text that describes or explains the purpose of the DB Alias.

Procedure Qualifier Enter a high-level qualifier for stored procedures. If blank, the entry on the **Stored Procedure Defaults** tab is used.

Procedure Action Select options to create/refresh procedures or use existing procedures. To select an option, click in the grid cell and click the down arrow.

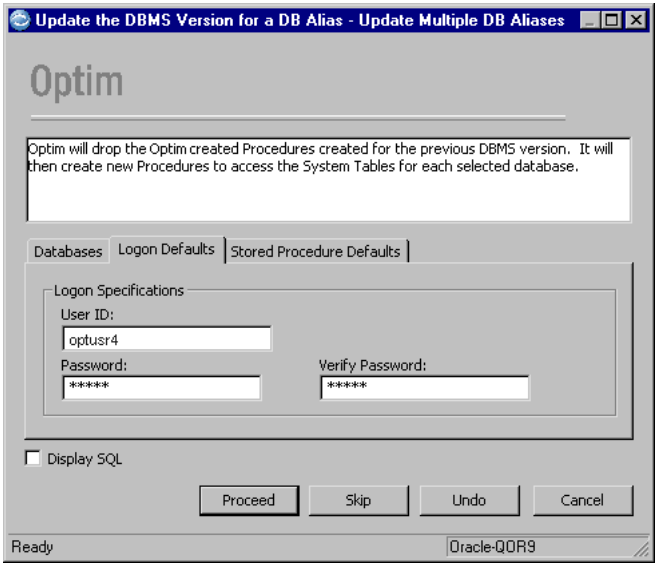
Grant Auth ID Enter an identifier for authorized users to maintain stored procedures. Specify a User ID, Group Name, or **Public**. If blank, the entry on the **Stored Procedure Defaults** tab is used.

Logon User ID Specify an identifier (up to 30 characters) required to logon to the DB Alias to create/refresh stored procedures. If blank, the entry on the **Logon Defaults** tab is used.

Logon Password	Enter a password (up to 30 characters) required to logon to the DB Alias to create/ refresh stored procedures. If blank, the entry on the **Logon Defaults** tab is used.
Display SQL	Select this check box to display SQL statements before dropping or creating stored procedures.

Logon Defaults Tab

Use the **Logon Defaults** tab to specify the **User ID** and **Password** needed to create/refresh stored procedures.

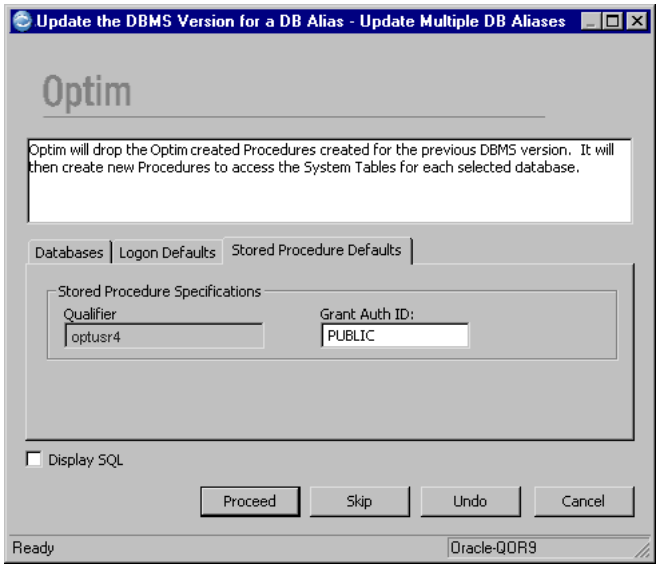


The entries on the **Logon Defaults** tab allow you to connect to the database while configuring workstations. Enter your password twice; the second time is for verification.

Note: The default logon information applies to all DB Aliases unless you provide explicit logon information on the **Databases** tab.

Stored Procedure Defaults

Use the stored procedure **Defaults** tab to specify the procedure **Qualifier** and **Grant Auth ID** required to drop and create stored procedures.



Note: The stored procedure defaults apply to all DB Aliases unless you provide explicit stored procedure information on the **Databases** tab.

When you specify the necessary information on each tab and click **Proceed**, the **Configuration** program connects to the first selected database. If the connection is successful, the update process drops the old stored packages, plans, or procedures, creates new ones, and updates the database signature. These steps are repeated for each selected database. When the process is complete, the **Complete** dialog displays.

7.12 Configure Options

The Product Configuration File contains the Product Options that apply to all users of ***Optim*** at a site. Personal Options are recorded in the workstation registry. Typically, the Product Configuration File and the Personal Options registry entries are created when you configure the first and additional workstations. However, you modify these options by selecting **Configure Options** from the **Tasks** menu.

Specify Optim Directory

Use the **Specify Optim Directory** dialog (see page 185) to select the name of the ***Optim*** Directory. Click **Proceed** to open the next dialog in the process.

Connect to Database

You can specify different Personal Options for each database. Therefore, the **Configuration** program may prompt you to connect to the database before proceeding. The **Connect to Database** dialog prompts for the **User ID**, **Password**, and **Connection String** needed to connect to the database for which Personal Options are specified.

Initialize Security

If ***Optim*** Security for the ***Optim*** Directory is not initialized, the **Initialize Security** dialog is displayed. Use this dialog to assign a Security Administrator and initialize ***Optim*** Security for the Directory. For more information about this dialog and initializing ***Optim*** Security, see **5.1.4 Optim Security** on page 128.

Change Security Administrator

If ***Optim*** Security for the ***Optim*** Directory is initialized, the **Change Security Administrator** dialog is displayed. Use this dialog to change the Security Administrator for the Directory. For more information about this dialog, see **7.4.2 Initialize Security or Change Security Administrator**.

Enable/Disable Optim Server Feature

On the **Enable/Disable the Optim Server Feature** dialog, specify whether to enable or disable the current machine as a ***Server***. If the site is not licensed for the ***Server***, **Enable** is not available.

Enable Disable Archive ODBC Feature

On the **Enable/Disable the Archive ODBC Feature** dialog, specify whether to enable or disable the ODBC driver. If the site is not licensed for ***Archive***, **Enable** is not available.

Specify Configuration File

In order to create the Product Configuration File, you must provide the fully qualified name of the file. The **Specify Product Configuration File** dialog prompts for this information. Refer to **5.1.5 Configure Options** on page 132 for additional information.

7.13 Create Primary Keys

If you add tables to a database, you may use the **Configuration** program to create ***Optim*** Primary Keys for tables that do not have DBMS primary keys, but do have unique indexes. When you create ***Optim*** Primary Keys, you must specify the ***Optim*** Directory and the DB Alias for the database where the tables reside.

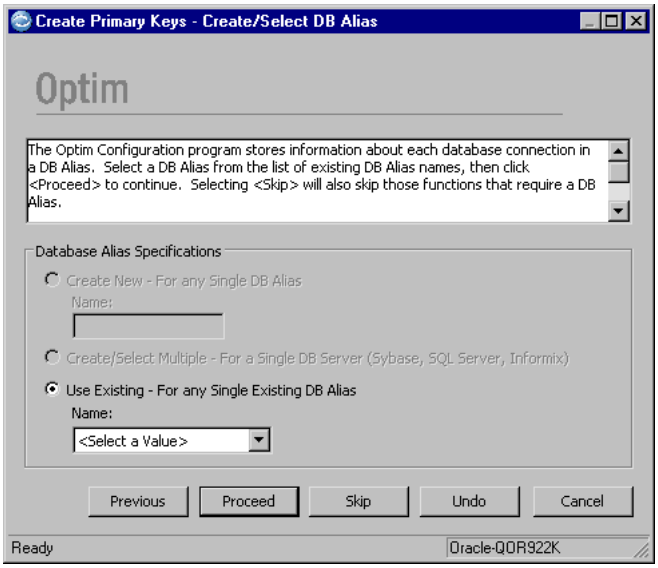
Optim Primary Keys are usually created when you configure the first workstation or when you create a DB Alias. After you install ***Optim***, you can create these primary keys by selecting **Create Primary Keys** from the **Tasks** menu, or by selecting **Configuration Assistant** from the **Help** menu.

Specify Optim Directory

Use the **Specify Optim Directory** dialog (see page 185) to select the name of the ***Optim*** Directory. Click **Proceed** to open the next dialog in the process.

Create/Select DB Alias

Use the **Create/Select DB Alias** dialog to specify the DB Alias for the database where you want to create Primary Keys.


Create Primary Keys - Create/Select DB Alias
Optim
The Optim Configuration program stores information about each database connection in a DB Alias. Select a DB Alias from the list of existing DB Alias names, then click <Proceed> to continue. Selecting <Skip> will also skip those functions that require a DB Alias.
Database Alias Specifications
Create New - For any Single DB Alias
Name:
Create/Select Multiple - For a Single DB Server (Sybase, SQL Server, Informix)
Use Existing - For any Single Existing DB Alias
Name:
<Select a Value>
Previous
Proceed
Skip
Undo
Cancel
Ready
Oracle-QOR922K

Create Primary Keys

The **Create Primary Keys** and **Select Primary Keys** dialogs allow you to create the ***Optim*** Primary Keys. Refer to **Create Primary Keys** on page 110.

Create Primary Keys for Another?

After you create the ***Optim*** Primary Keys for tables accessed using a particular DB Alias, the **Configuration** program prompts you to create Primary Keys for tables accessed using a different DB Alias. To continue, click **Proceed**.

- If you select **Create Primary Keys for another DB Alias**, the **Create/Select DB Alias** dialog opens to repeat the sequence.
- If you clear **Create Primary Keys for another DB Alias**, the **Configuration** program completes the **Create Primary Keys** process and returns to the main window.

7.14 Create Copies of DB2 z/OS Relationships

To facilitate use of ***Optim*** with DB2 z/OS tables, copy the DB2 relationships into the ***Optim*** Directory to reduce the run time when accessing DB2 tables. The **Configuration** program provides an option to copy these relationships to the ***Optim*** Directory. You can start this process by selecting **Create Copies of DB2 MVS Relationships** from the **Tasks** menu, or by selecting the **Configuration Assistant** from the **Help** menu.

Specify Optim Directory

Use the **Specify Optim Directory** dialog (see page 185) to select the name of the ***Optim*** Directory. Click **Proceed** to open the next dialog in the process.

Create/Select DB Alias

Use the **Create/Select DB Alias** dialog (see page 207) to specify the DB Alias for the DB2 z/OS database where the relationships are to be copied. Click **Proceed** to open the next dialog.

Not a DB2 for MVS Database

If you select a DB Alias for a database that is not a DB2 z/OS database, the **Configuration** program displays the **Not a DB2 for MVS Database** dialog. This dialog prompts you to return to the **Create/Select DB Alias** dialog, using **Previous**, to select another DB Alias. To continue, click **Proceed**.

Create Copies of DB2 MVS Relationships?

If you select a DB Alias for a DB2 z/OS database, the **Configuration** program prompts you to confirm that relationships are to be copied, using the **Create Copies of DB2 MVS Relationships?** dialog. Select the check box and click **Proceed** to copy the relationships to the ***Optim*** Directory.

Create Copies for Another?

After the DB2 z/OS relationships are copied to the ***Optim*** Directory, the **Configuration** program prompts you to copy relationships for another DB Alias. If so, the **Create/Select DB Alias** dialog opens, allowing you to choose another DB Alias. If not, the process completes.

7.15 Load/Drop Sample Data

Sample tables are distributed with ***Optim***. Generally, you load this sample data when you configure the first workstation, however, you can load it independently or when you configure an additional workstation.

You can load, refresh, or drop sample data by selecting the **Load/Drop Sample Data** option, which guides you through the process. You can start this process by selecting **Load/Drop Sample Data** from the **Tasks** menu, or by selecting the **Configuration Assistant** from the **Help** menu.

Specify Optim Directory

A DB Alias is required to access the sample tables. The DB Alias, used as a high-level qualifier for the table names, provides a single-name association for parameters needed to connect to the database. The DB Alias and other ***Optim*** objects, created when the sample tables are created, are stored in an ***Optim*** Directory.

Use the **Specify Optim Directory** dialog (see page 185) to select the name of the ***Optim*** Directory. Click **Proceed** to open the next dialog.

Create/Select DB Alias

Use the **Create/Select DB Alias** dialog (see page 207) to specify the DB Alias for the sample tables. Click **Proceed** to open the next dialog.

Load/Drop Sample Tables

After you select the DB Alias for the sample tables, the **Configuration** program opens the **Load/Drop Sample Tables** dialog. If you are creating or refreshing the tables, you must specify an identifier (**Creator ID**, **Schema Name**, or **Owner ID**) and **Tablespace**. If you are dropping sample tables, only the identifier is required. Refer to **Load/Drop Sample Tables** on page 112.

Load/Drop Sample Data for Another DB Alias

After you load or drop sample tables associated with a particular DB Alias, the **Configuration** program displays the **Load/Drop Sample Data for Another DB Alias** dialog and prompt you to load or drop sample tables associated with a different DB Alias. If so, the **Create/Select DB Alias** dialog opens to restart the process. Otherwise, the process completes and returns to the main window.

7.16 Load/Drop Data Privacy Data

Data privacy data tables are available to clients who have an ***Optim*** Data Privacy License. These tables allow you to mask company and personal data — such as employee names, customer names, social security numbers, credit card numbers, and e-mail addresses — to generate transformed data that is both valid and unique. Generally, these data privacy tables are loaded when you configure the first workstation, but you also can load them independently or when you configure an additional workstation.

You can load, refresh, or drop data privacy data by selecting the **Load/Drop Data Privacy Data** option, which guides you through the process. You can start this process by selecting **Load/Drop Data Privacy Data** from the **Tasks** menu, or by selecting the **Configuration Assistant** from the **Help** menu.

Specify Optim Directory

A DB Alias is required to access the data privacy tables. The DB Alias, used as a high-level qualifier for the table names, provides a single-name association for parameters needed to connect to the database. The DB Alias and other ***Optim*** objects, created when the data privacy tables are created, are stored in an ***Optim*** Directory.

Use the **Specify Optim Directory** dialog (see page 185) to select the name of the ***Optim*** Directory. Click **Proceed** to open the next dialog.

Create/Select DB Alias

Use the **Create/Select DB Alias** dialog (see page 207) to specify the DB Alias for the data privacy tables. Click **Proceed** to open the next dialog.

Load/Drop Data Privacy Tables

After you select the DB Alias for the data privacy tables, the **Configuration** program opens the **Load/Drop Data Privacy Tables** dialog. If you are creating or refreshing the tables, you must specify an identifier (**Creator ID**, **Schema Name**, or **Owner ID**) and **Tablespace**. If you are dropping data privacy tables, only the identifier is required. Refer to **Load/Drop Data Privacy Tables** on page 115.

Load/Drop Data Privacy Data for Another DB Alias

After you load or drop sample data privacy tables associated with a particular DB Alias, the **Configuration** program displays the **Load/Drop Data Privacy Data for Another DB Alias** dialog and prompts you to load or drop the data privacy tables associated with a different DB Alias. If so, the **Create/Select DB Alias** dialog opens to restart the process. Otherwise, the process completes and returns to the main window.

7.17 Drop DB Alias or Optim Tables

At times it may be necessary to drop a DB Alias or an ***Optim*** Directory. Use **Drop DB Alias or Optim Tables** to guide you in performing one or both tasks. The following guidelines apply.

- When you drop a DB Alias, ***Optim*** can no longer access data in that database, and any ***Optim*** objects that refer to the DB Alias are invalid. However, you can recreate the DB Alias and restore access to the database and ***Optim*** objects.
- When you drop an ***Optim*** Directory, the DB Aliases and other ***Optim*** objects stored in the Directory cannot be recovered.

Specify Optim Directory

Use the **Specify Optim Directory** dialog (see page 185) to select the name of the ***Optim*** Directory that stores the DB Alias you want to drop or to specify the ***Optim*** Directory you want to drop. Click **Proceed** to open the next dialog.

Connect to Database

Optim must connect to the database to drop the ***Optim*** Directory tables and packages, plans, or procedures. Use the **Connect to Database** dialog (see page 205) to specify the connection information.

Create/Select DB Alias

Use the **Create/Select DB Alias** dialog (see page 207) to specify a DB Alias you want to drop. Click **Proceed** to drop the DB Alias, or click **Skip** to open the **Drop Optim Directory?** dialog, which you can use to drop the specified ***Optim*** Directory, including all DB Aliases and other objects stored in it.

Load/Drop Sample Tables

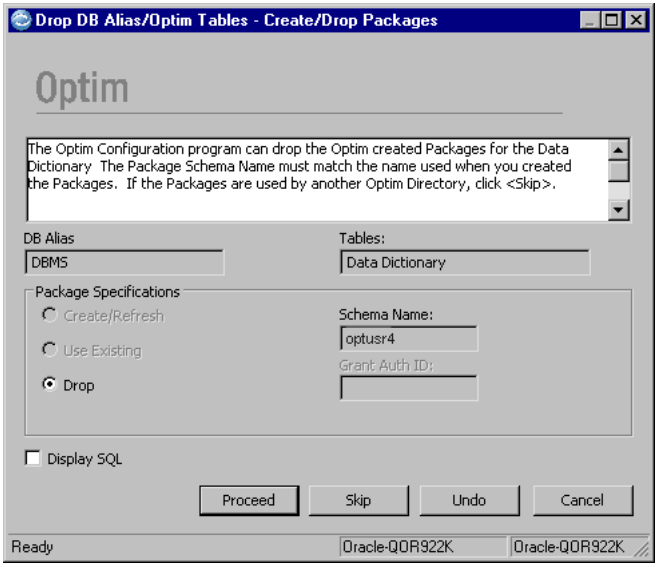
The **Load/Drop Sample Tables** dialog prompts you to specify the identifier (**Creator ID**, **Schema Name**, or **Owner ID**) for the sample tables to be dropped. Refer to **Load/Drop Sample Tables** on page 112.

Load/Drop Data Privacy Tables

If you have an ***Optim*** Data Privacy License, the **Load/Drop Data Privacy Tables** dialog prompts you to specify the identifier (**Creator ID**, **Schema Name**, or **Owner ID**) for the data privacy tables to be dropped. Refer to **Load/Drop Data Privacy Tables** on page 115.

Drop Packages

Before dropping packages, plans, or procedures used to access the database, the **Configuration** program displays the **Create/Drop Packages**, **Bind/Drop Plans**, or **Create/Drop Stored Procedures** dialog, as appropriate.



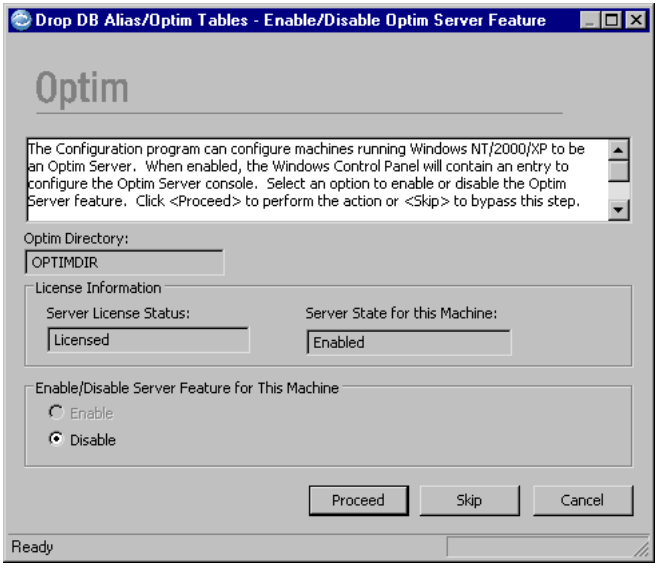
To retain the packages, plans, or procedures, click **Skip**. To browse the DDL used to drop the packages, plans, or procedures, select **Display SQL** and click **Proceed**.

Drop Another DB Alias?

After you drop the DB Alias, the **Configuration** program opens the **Drop Another DB Alias?** dialog. Select the check box to open the **Create/Select DB Alias** dialog and restart the process for another DB Alias.

Disable the Optim Server Feature

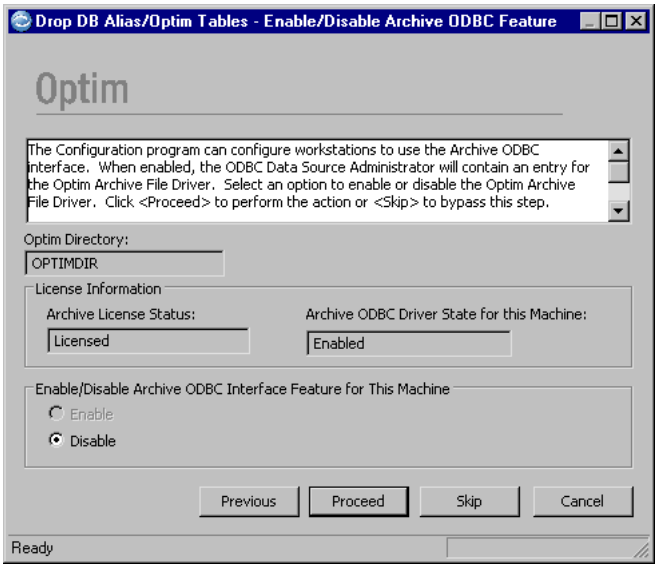
The **Configuration** program opens the **Enable/Disable Optim Server Feature** dialog next, to allow you to disable the ***Server*** feature.


Drop DB Alias/Optim Tables - Enable/Disable Optim Server Feature
Optim
The Configuration program can configure machines running Windows NT/2000/XP to be an Optim Server. When enabled, the Windows Control Panel will contain an entry to configure the Optim Server console. Select an option to enable or disable the Optim Server feature. Click <Proceed> to perform the action or <Skip> to bypass this step.
Optim Directory:
OPTIMDIR
License Information
Server License Status:
Licensed
Server State for this Machine:
Enabled
Enable/Disable Server Feature for This Machine
Enable
Disable
Proceed
Skip
Cancel
Ready

Click **Proceed** to disable the ***Server*** feature, or click **Skip** to advance to the next step without disabling the ***Server*** feature. If the site is not licensed for the ***Server***, this dialog is not displayed.

Disable the Archive ODBC Feature

The **Configuration** program opens the **Enable/Disable Archive ODBC Feature** dialog next. This dialog allows you to disable the **Archive ODBC** interface feature.


Drop DB Alias/Optim Tables - Enable/Disable Archive ODBC Feature
Optim
The Configuration program can configure workstations to use the Archive ODBC interface. When enabled, the ODBC Data Source Administrator will contain an entry for the Optim Archive File Driver. Select an option to enable or disable the Optim Archive File Driver. Click <Proceed> to perform the action or <Skip> to bypass this step.
Optim Directory:
OPTIMDIR
License Information
Archive License Status:
Licensed
Archive ODBC Driver State for this Machine:
Enabled
Enable/Disable Archive ODBC Interface Feature for This Machine
Enable
Disable
Previous
Proceed
Skip
Cancel
Ready

Click **Proceed** to disable the **Archive ODBC** feature, or click **Skip** to advance to the next step without disabling the **Archive ODBC** feature. If the site is not licensed for ***Archive***, this dialog is not displayed.

7.17.1 Drop the Optim Directory?

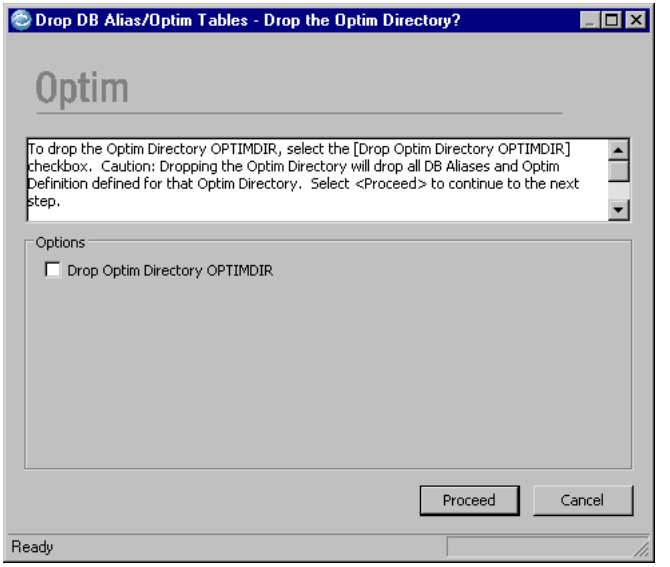
If you do not drop another DB Alias, the **Configuration** program opens the **Drop the Optim Directory** dialog. Select the check box to drop the ***Optim*** Directory.

Connect to Database

Optim must connect to the database in order to drop the ***Optim*** Directory tables and packages, plans, or procedures. Use the **Connect to Database** dialog (see page 205) to specify the connection information.

Drop Optim Directory Tables

Before you drop an ***Optim*** Directory (and ***Optim*** Directory tables), the **Configuration** program displays the table identifier and prompts you to review the generated DDL, using the **Drop Optim Directory Tables** dialog.


Drop DB Alias/Optim Tables - Drop the Optim Directory?
Optim
To drop the Optim Directory OPTIMDIR, select the [Drop Optim Directory OPTIMDIR] checkbox. Caution: Dropping the Optim Directory will drop all DB Aliases and Optim Definition defined for that Optim Directory. Select <Proceed> to continue to the next step.
Options
Drop Optim Directory OPTIMDIR
Proceed
Cancel
Ready

To retain the ***Optim*** Directory tables and objects in it, click **Skip**.

Create/Drop Packages

When you drop an ***Optim*** Directory, all objects stored in that Directory are deleted. For this reason, the packages, plans, or procedures used to access the ***Optim*** Directory are no longer useful and should be dropped. The **Create/Drop Packages**, **Bind/Drop Plans**, or **Create/Drop Stored Procedures** dialog prompts you to do this.

Drop Another Optim Directory?

After you drop the ***Optim*** Directory, the **Configuration** program opens the **Drop Another Optim Directory?** dialog. Select the check box to restart the process for another ***Optim*** Directory.

7.18 Purge Optim Directory Registry Entry

For security or other reasons, you may want to purge the Windows registry entry for an ***Optim*** Directory from a workstation, but not drop the Directory or packages, plans, or procedures used to access that Directory. For example, when you remove an ***Optim*** Directory from a multi-user environment, you can purge the ***Optim*** Directory registry entry from each workstation. In addition, you can disable ***Optim*** for any workstation, simply by purging the registry entry.

When you select **Purge Optim Directory Registry Entry** from the **Tasks** menu, the **Configuration** program opens a dialog explaining the process and prompting you to confirm that you want to purge the registry entry for access to the ***Optim*** Directory rather than drop the ***Optim*** Directory. Select the check box to purge the registry entry.

Note: To reinstate a purged ***Optim*** Directory, refer to **7.3 Access Existing Optim Directory**.

Purge a Pre-6.0 Optim Directory Entry

After you confirm that you want to purge an ***Optim*** Directory entry, the **Configuration** program prompts you to indicate the version of the registry entry you want to purge. Select **Purge a pre-6.0 Optim Registry Entry** to purge an ***Optim*** Directory registry entry created before version 6.0. To purge an ***Optim*** Directory registry entry created with version 6.0 or later, leave this option blank. Click **Proceed** to open the next dialog.

Specify Optim Directory

After you confirm the version of the ***Optim*** Directory entry you want to purge, the **Configuration** program opens the **Specify Optim Directory** dialog (see page 185). Use this dialog to provide the name of the ***Optim*** Directory for the Windows registry entry you want to purge. Click **Proceed** to open the next dialog.

Confirm Purge Optim Registry Entry?

After you select the ***Optim*** Directory for the registry entry you want to purge, the **Configuration** program prompts you to confirm the Directory name. Select the check box and click **Proceed** to purge the registry entry for the named ***Optim*** Directory. Next, the **Configuration** program opens a query dialog that prompts you to purge the registry entry for another ***Optim*** Directory. To purge another, select the check box and click **Proceed** to open the **Specify Optim Directory** dialog and select another ***Optim*** Directory.

7.19 Purge DB Alias

Select **Purge DB Alias** from the **Tasks** menu to delete a DB Alias from an ***Optim*** Directory without connecting to the database. This task does not drop packages, plans, or procedures created with the DB Alias, nor does it drop sample or other tables accessed using the DB Alias.

You may purge a DB Alias any time you drop a database; for example, when a database used for testing applications is dropped after testing is completed. You may also purge a DB Alias to make a database temporarily inaccessible to the workstations using ***Optim***.

Note: To reinstate a purged DB Alias, refer to **7.1 Create/Update DB Alias**.

Specify Optim Directory

Use the **Specify Optim Directory** dialog (see page 185) to select the name of the ***Optim*** Directory in which the DB Alias entry you want to purge is located. Click **Proceed** to open the next dialog.

Create/Select DB Alias

Use the **Create/Select DB Alias** dialog (see page 207) to specify a DB Alias to purge. Click **Proceed** to open the next dialog.

Confirm Purge DB Alias?

After you select a DB alias to purge, the **Configuration** program prompts you to confirm the selected DB Alias is to be dropped. This option is selected when the dialog opens. Click **Proceed** to continue. Next, the **Configuration** program opens a query dialog that prompts you to purge another DB Alias. To purge another DB Alias, select the check box and click **Proceed** to open the **Create/Select DB Alias** dialog on which you can select another DB Alias.

8. Product Options

Each workstation using ***Optim*** must reference a Product Configuration File. The path to the appropriate Product Configuration File is specified in Personal Options. You must use the **Product Options** dialog, however, to create a Product Configuration File.

Note: A password is required to open the **Product Options** dialog.

Generally, Product Options parameters enforce site and system requirements. Use the **Product Options** dialog to:

- Name the Product Configuration File.
- Establish password security for Product Options.
- Limit the amount of data that can be processed at one time.
- Define defaults and user control over certain activities.
- Provide connection information for machines hosting the ***Optim Server*** (***Server***).
- Specify general parameters for editing or archiving.
- Customize loader parameters and enforce loader requirements.

8.1 Open the Product Options Editor

You can configure Product Options using the **Configuration** program, or you can set options within ***Optim***.

Using the Configuration program

To Configure Product Options using the Configuration program:

1. Open the **Optim Configuration** component.
2. In the main window, select **Configure Options** from the **Tasks** menu.
3. Specify an Optim Directory and click **Proceed.**
4. Click **Skip** on the **Initialize Security/Change Security Administrator**, **Enable/Disable the Optim Server Feature**, and **Enable/Disable the Archive ODBC Feature** dialogs to open the **Specify Product Configuration File** dialog.
5. Select **Create New File** or **Use Existing File**, verify the name of the Configuration File, and click **Proceed** to open the **Modify Product Options** dialog.
6. Click **Product Options** to open the **Enter Product Options Password** dialog.
7. Specify the case-sensitive password to open the **Product Options** dialog. (The initial password is *optim*.)
8. Enter the necessary details on each tab in Product Options.
9. Choose one of the following:
   - To close the **Product Options** dialog without saving your changes, click **Cancel**.
   - To save your changes and continue using the **Product Options** dialog, click **Apply**.
   - To save your changes and close the **Product Options** dialog, click **OK** to return to the **Modify Product Options** dialog.
10. Click **Proceed** to open the **Modify Personal Options** dialog.

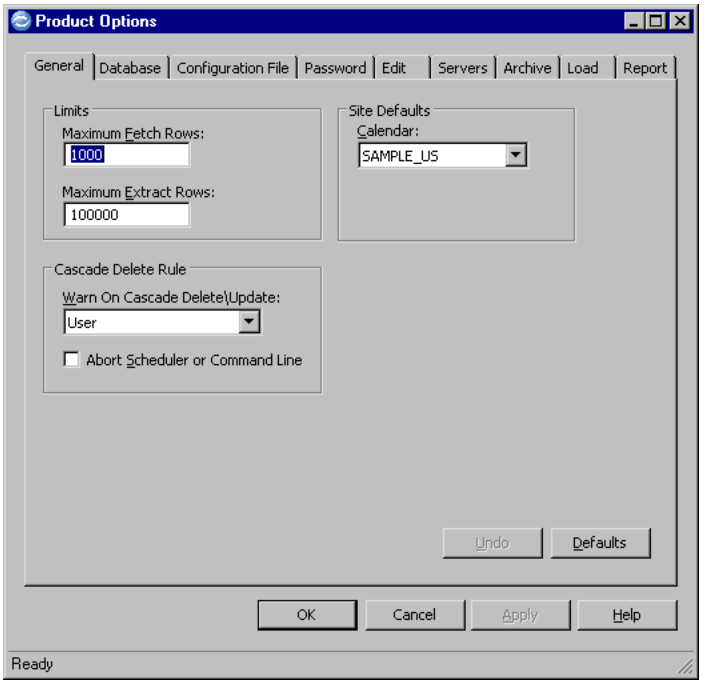
Within Optim

To Configure Product Options within Optim:

1. In the main window, select **Product** from the **Options** menu to open the **Enter Product Options Password** dialog.
2. Specify the case-sensitive password to open the **Product Options** dialog. (The initial distributed password is *optim*.)
3. Specify the necessary details on each tab in Product Options.
4. Choose one of the following:
   - Click **Cancel** to close the **Product Options** dialog without saving your changes.
   - Click **Apply** to save your changes and continue using the **Product Options** dialog.
   - Click **OK** to save your changes and close the **Product Options** dialog.

8.2 Using the Editor

The **Product Options** dialog allows you to customize various features and display options in ***Optim***. Several tabs in the **Product Options** dialog allow you to review and set the options as required.



Tabs

The tabs in the **Product Options** dialog are described briefly in the following paragraphs. Detailed information is provided in each section of this chapter.

General Establish the maximum number of rows that can be read from a table when browsing or editing table data or using Point and Shoot, and the maximum number of rows that can be extracted or archived during a single process. Also, choose a default Calendar and set cascade delete/update options. (The **General** tab is always foremost when the dialog opens.)

Database	Establish the maximum number of rows that can be processed in an Insert or Delete Process before a *commit* is issued, and prevent or allow optional table locks during an Insert or Delete Process.
Configuration File	Establish the path to the Configuration File for the selected Product Options.
Password	Change the password for the **Product Options** dialog.
Edit	Select audit preferences for editing data. Specify other site options for using default values.
Servers	Specify protocol, endpoint address, and network information for machines configured with the ***Server***.
Archive	Select options that apply to Archive Processes.
Load	Specify options for adding Loader parameters.
Report	Specify defaults for creating reports using the **Report Request Editor**, including limits and spacing preferences.

8.2.1 General Tab

Use the **General** tab to establish default fetch and extract limits for Archive, Compare, Edit, and Extract Processes.

Limits

Establish the maximum number of rows in a fetch set for browsing or editing data or using Point and Shoot, and the maximum number of rows for extracting or archiving data.

Maximum Fetch Rows	Specify the maximum number of rows (1 to 100000) retrieved from a table. This limit applies to rows that are fetched to browse or edit table data or for Point and Shoot. If you do not specify a value, the default value is 1000. A user can establish a lower **Maximum Fetch Rows** limit by selecting **Personal** from the **Options** menu and editing the **Display** tab.

Maximum Extract Rows

Specify the maximum number of rows (1 to 999999999) that can be processed during a single Extract or Archive Process. If you do not specify a value, the default value is 100000.

A **Row Limit** for an Archive or Extract Process cannot exceed this value.

Site Defaults

The site-specific, default Calendar used to schedule action requests or to age data in a Column Map.

Calendar

Select a site default Calendar. To select from a list of available calendars, click the down arrow. You can select a different calendar on a process request, as needed.

Cascade Delete Rule

Set options for performing a cascading delete or update on tables that are not explicitly included in an Access Definition or a process.

Warn on Cascade Delete/Update

Click the down arrow to choose when to display a warning if a cascading delete or update may occur.

User

Allow the user to determine when to display a warning. This is the default setting.

The corresponding **Warn on Cascade Delete/Update** setting in Personal Options is enabled. See **Warn on Cascade** on page 309 for more information.

Runtime

Display a cascade delete/update warning only at run time of a process.

The corresponding setting in Personal Options is unavailable and set to **Runtime**.

Saving Access Definition

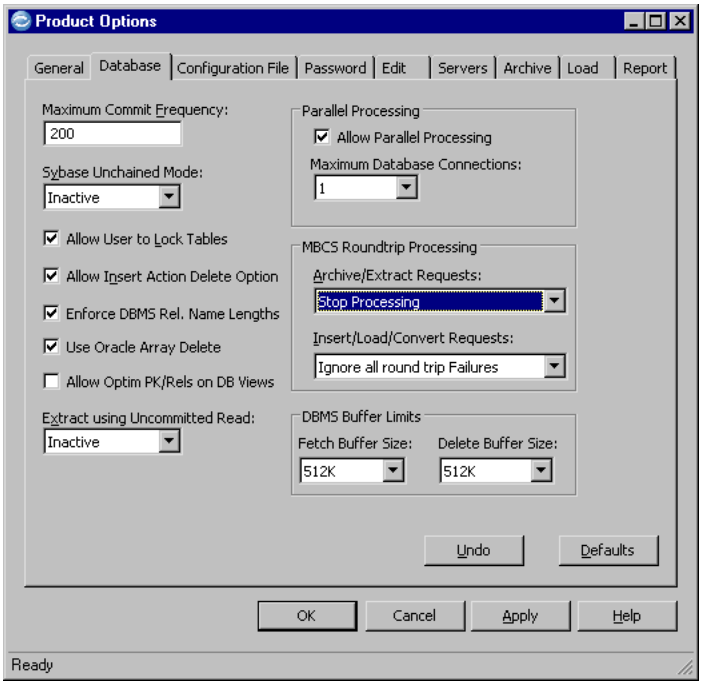
Display a cascade delete/update warning only when saving the Access Definition.

The corresponding setting in Personal Options is unavailable and set to **Saving Access Definition**.

	Always	Display a cascade delete/update warning at run time of a process, and when saving the Access Definition. The corresponding setting in Personal Options is unavailable and set to **Always**.
	Never	Do not display a cascade delete/update warning. The corresponding setting in Personal Options is unavailable and set to **Never**.
Abort Scheduler or Command Line	Select this check box to abort the process when run from the **Scheduler** or the Command Line Interface, and the cascade delete/update affects at least one table that is not explicitly included in the process. (This check box is selected by default.)	

8.2.2 Database Tab

Use the **Database** tab to manage database activity during Insert, Restore, and Delete Processes.



Maximum Commit Frequency

Specify the maximum number of rows (1 to 999999) inserted, restored, or deleted before changes are committed to the database. If you do not specify a limit, the default value is 200. An Insert, Restore, or Delete Request can require more frequent commits.

Sybase Unchained Mode

Optim normally runs in chained mode. When a trigger in a Sybase ASE table will be fired as a result of an Insert or Delete Process, and the trigger calls a stored procedure that must run in unchained mode, the connection must be in unchained mode for the procedure to work.

Select an option for running an Insert or Delete Process, as follows:

Active — Require Insert, Restore, and Delete Processes to run in unchained mode; the **Run in Unchained Mode** check box in Personal Options (see **Sybase Unchained Mode** on page 329) is unavailable.

Inactive	Set all processes to run in normal mode; the **Run in Unchained Mode** check box in Personal Options is unavailable.
Default Active	The **Run in Unchained Mode** check box in Personal Options is available and selected, by default. Insert, Restore, and Delete Processes run in unchained mode unless the **Run in Unchained Mode** check box in Personal Options is cleared.
Default Inactive	The **Run in Unchained Mode** check box in Personal Options is available and cleared, by default. Insert, Restore, and Delete Processes run in normal mode unless the **Run in Unchained Mode** check box in Personal Options is selected.

Allow User to Lock Tables

Select this check box to enable the **Lock Tables** option in the Insert, Restore, and Delete Request Editors. Users can then use the option to lock tables during an Insert, Restore, or Delete Process. Locking tables ensures that other database activity does not interfere with the process and prevents other users from accessing tables involved in the process.

Allow Insert Action Delete Option

Select this check box to enable the Delete Options box in the Insert Request Editor. If you clear this check box, the Delete Options box is unavailable, and the **Delete** option is set to **No Tables**, by default.

Enforce DBMS Rel. Name Lengths

Select this check box to enforce DBMS restrictions for relationship name length when creating or importing relationships. This option is selected by default. Clear this check box to override DBMS naming restrictions and create or import relationships with names (constraints) up to 64 characters. After changing this option, you must exit ***Optim*** before the change takes effect. You cannot create a DBMS relationship based on an Optim relationship with a name that exceeds the DBMS restrictions.

Use Oracle Array Delete

Select **Use Oracle Array Delete** to use the Oracle array delete feature during a Delete Process. This option is selected by default.

Note: If your site audits Delete processing, be aware that Array Delete may report rows as being successfully deleted that do not exist in the database and, therefore, were not actually deleted by the process.

The Oracle array delete feature is performed during a Delete Process only when the following are true:

- **Compare Row Contents** is not selected in the **Delete Request Editor**.
- Both the table in the source file and database have a unique primary key.
- The table has no file attachments to be deleted.

Allow Optim PK/Rels on DB Views

Select this check box to allow users to define **Optim** Primary Keys and Relationships for database views. Default?

Extract using Uncommitted Read

Set an option to enable extracting of uncommitted rows from the database during an Archive or Extract Process. You can extract uncommitted rows from specific tables in the Access Definition or all tables. Selecting this option for tables with known performance problems may increase the speed of your Archive or Extract processes.

Active	Automatically extract uncommitted rows from each table in the Access Definition during all Archive or Extract Processes. The **Uncommitted Read** check box on the Access Definition Editor is unavailable.
Inactive	Automatically extract only committed rows from each table in the Access Definition during all Archive or Extract Processes. The **Uncommitted Read** check box on the Access Definition Editor is unavailable.
Default Active	The **Uncommitted Read** option on the Access Definition Editor is available and selected by default. Uncommitted rows are extracted from the table unless the **Uncommitted Read** check box is cleared.
Default Inactive	The **Uncommitted Read** option on the Access Definition Editor is available and cleared by default. Uncommitted rows are not extracted from the table unless the **Uncommitted Read** check box is cleared.

Notes:

- If you choose to extract uncommitted rows, the relational integrity of the data in the Archive or Extract File may be

compromised. Use caution if inserting data from any Archive or Extract File with uncommitted rows.

- ***Optim*** disables the extracting of uncommitted rows if the DBMS or version does not support it, regardless of the setting.

Parallel Processing

Set options to determine the maximum number of concurrent database connections allowed. Increasing database connections improves performance when processing large quantities of data by allowing multiple threads to process rows in parallel.

Allow Parallel Processing

Select this check box to enable **Maximum Database Connections**.

Maximum Database Connections

Increase the maximum number of concurrent database connections for an Archive, Extract, or Delete Process. You can select an even number of maximum database connections. from 2 though 32, or **Maximum**. Your selection enables **Database Connections** on the Archive, Extract, and Delete Request Editors and **Maximum Database Connections** in Personal Options (see **Maximum Database Connections** on page 327).

MBCS Roundtrip Processing

Options for handling characters that could cause round trip conversion issues in a multi-byte ***Optim*** Directory or DB Alias.

Optim uses the Unicode character set in dialogs and to process data. In some multi-byte character sets (such as Oracle JA16SJIS), multiple characters are mapped to the same Unicode character. When these characters are converted from Unicode back to multi-byte (a round trip), the original character may not be returned.

Archive/Extract Requests

Select an option for handling round trip conversion issues during Archive or Extract processing:

Stop Processing

Stop processing when a multi-byte character is encountered that could cause an incorrect round trip conversion. Each row of data is checked for characters that could cause an incorrect round trip conversion.

	Ignore all round trip Failures	Continue processing when a multi-byte character is encountered that could cause an incorrect round trip conversion. (Default.)
	Use Value from Personal Options	Use the round trip processing setting from the **Database** tab in Personal Options.
Insert/Load/ Convert Requests	Select an option for handling round trip conversion issues during Insert, Load, or Convert processing:	
	Stop Processing	Stop processing when a multi-byte character is encountered that could cause an incorrect round trip conversion. Each row of data is checked for characters that could cause an incorrect round trip conversion.
	Ignore all round trip Failures	Continue processing when a multi-byte character is encountered that could cause an incorrect round trip conversion. (Default.)
	Use Value from Personal Options	Use the round trip processing setting from the **Database** tab in Personal Options.

Select the **Ignore all round trip Failures** option if the database does not contain data with characters that could cause an incorrect round trip conversion, or if columns used to manipulate data in a Column Map (e.g., a function is used) and columns for which selection criteria are defined do not contain characters that could cause an incorrect round trip conversion.

DBMS Buffer Limits

Set the buffer size to use when fetching or deleting rows from the database. ***Optim*** multiplies the specification for Fetch Buffer Size or Delete Buffer Size by the value for **Maximum Database Connections.**

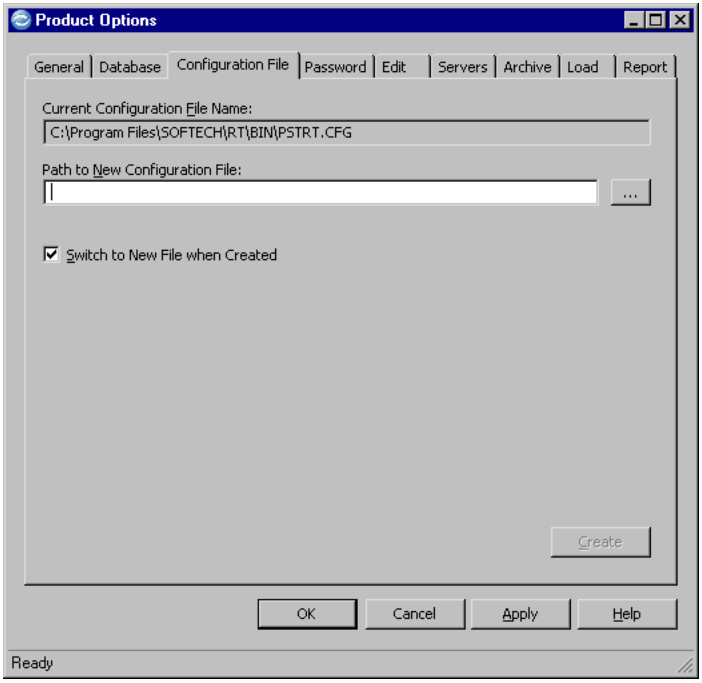
You can select a value from 64K to 1024K, in increments of 32. Use the default value unless you are processing tables larger than 10,000 rows.

Fetch Buffer Size Size of the buffer used when rows are fetched from the database. The default is 512K.

Delete Buffer Size Size of the buffer used when rows are deleted from the database. The default is 512K.

8.2.3 Configuration File Tab

Use the **Configuration File** tab to review the path for the current Configuration File and set new Configuration File preferences.



Current Configuration File Name Directory path and name of the Configuration File that ***Optim*** is currently using.

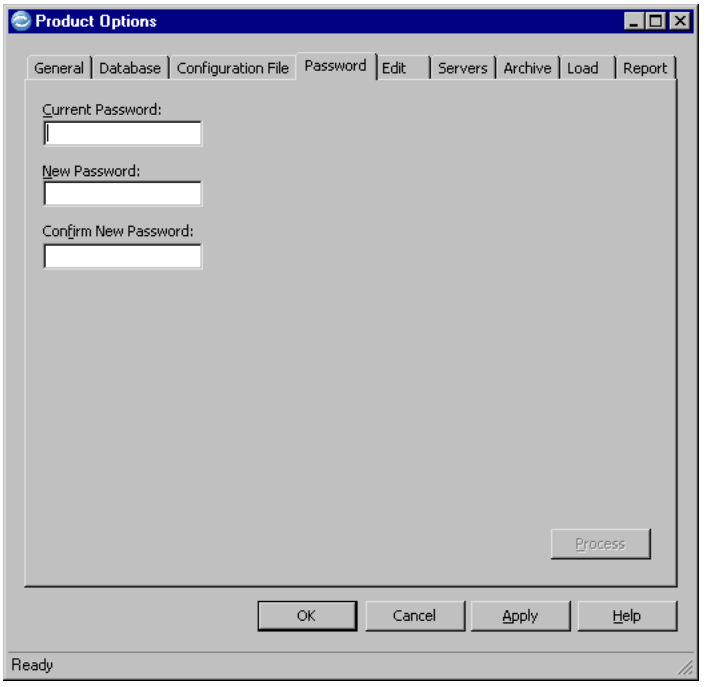
Path to New Configuration File Specify the directory path for a new or different Configuration File. To select an existing Configuration File from your system directories, click the browse button. To create a new Configuration File, specify the directory path and file name and then click **Create**. If you do not

specify a full directory path with the file name, the current drive and directory are used.

Switch to New File when Created Select this check box to apply the new Configuration File as soon as it is created. Do not select this check box if you intend to modify the current Product Options and want to retain the original Configuration File.

8.2.4 Password Tab

Use the **Password** tab to change the password needed to access Product Options.



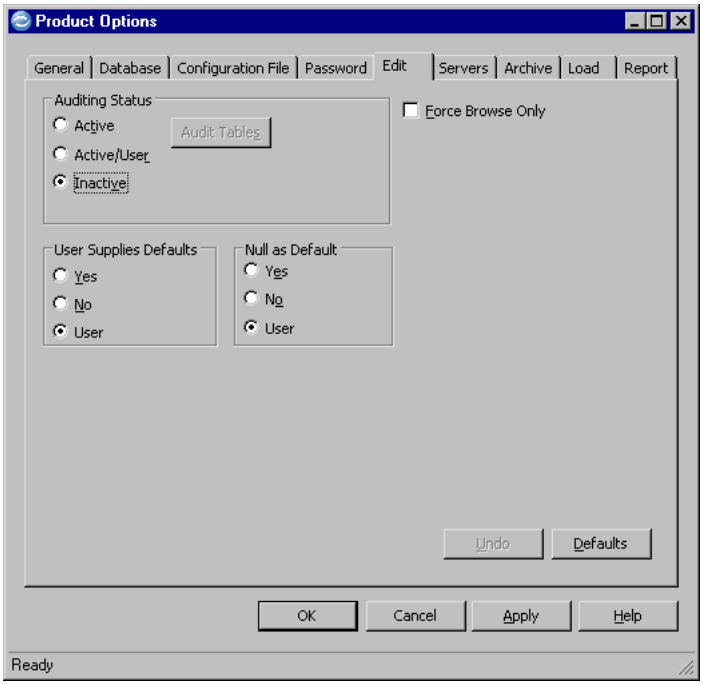
Current Password Enter the current password (1 to 8 characters). Passwords are case sensitive. Initially, this password is *optim*.

New Password Enter the new password (1 to 8 characters, case-sensitive). For security reasons, the password is displayed as a series of asterisks (****).

Confirm New Password Confirm the new password by entering it a second time. For security reasons, the password is displayed as a series of asterisks (****).

8.2.5 Edit Tab

Use the **Edit** tab to select audit preferences for editing data and specify other site options for using default values.



Auditing Status

Activate auditing to record rows that you edit and store images of unedited rows in an ***Optim*** Directory table. You can browse these rows, establish the period of time for which they are stored rows, and limit the number of rows retained. When rows of audit information expire, they are automatically deleted. When the maximum number of rows is exceeded, the oldest rows are deleted to make space for new rows.

Active Select this option to enable the auditing feature at the site level. Click **Audit Tables** to open a dialog on which you can select tables to be audited on a site basis.

Active/User Select this option to activate auditing at the site level and allow users to establish auditing for the workstation. Click **Audit Tables** to open a dialog on which you can select tables to be audited on a site basis.

This option enables the auditing feature in Personal Options (see **Auditing Active** on page 310). Users can select additional tables to audit, but cannot disable auditing for tables audited on a site basis.

Inactive Select this option to disable the auditing feature. No users can audit.

User Supplies Defaults

Choose whether to require user-supplied values in columns that cannot accept default values. This option applies to new rows that a user inserts while editing a database table.

Note: ***Optim*** can provide a default value according to the data type. Possible values include blank, NULL, zero, current date, current time, or current timestamp.

Yes Select this option to require a user-supplied value for every column that cannot accept a default value. If you select this option, the **User Supplies Defaults** check box in Personal Options (or Edit Preferences for the Table Editor) is unavailable. See **User Supplies Defaults** on page 309 for more information.

No Select this option if your site does not require user-supplied values for columns that cannot accept a default value.

User Select this option to allow users to supply a value for any column that cannot accept a default value. If you select this option, users can modify this selection in Personal Options (or Edit Preferences in the Table Editor).

Null as Default

Choose whether to use the NULL character as the default value for nullable columns. This option applies to new rows that a user inserts while editing a database table.

Note: ***Optim*** can provide a default value based on the column data type. Other than NULL, possible values include blank, zero, current date, current time, and current timestamp.

Yes Select this option to display the NULL character as the default value for nullable columns when editing data. If you select this option, users cannot modify this selection in Personal Options (or Edit Preferences in the Table Editor). See **Display NULL as Insert Default** on page 309 for more information.

No Select this option if your site prefers not to display the NULL character as the default value for nullable columns while editing data.

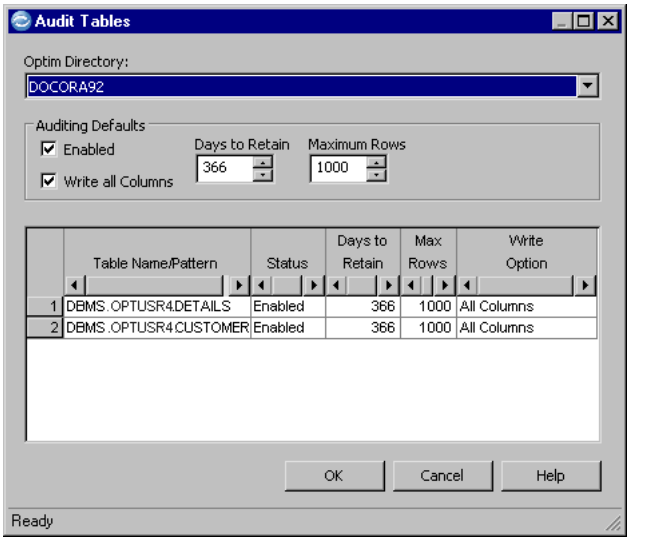
User Select this option to allow users to display the NULL character as the default value for nullable columns while editing data. If you select this option, users can modify this selection in Personal Options (or Edit Preferences in the Table Editor).

Force Browse Only

Select this check box to force all new and existing Edit Definitions to be in Browse Only mode. When you select this check box, edit options on the **Edit** tab in Personal Options and the Edit Preferences on the Table Editor are unavailable. (For example, the option for **Undo Levels** is unavailable, because Undo entries are not created in Browse Only mode.)

Audit Tables Dialog

If you select **Active** or **Active/User** on the **Edit** tab of the **Product Options** dialog, click **Audit Tables** to display the **Audit Tables** dialog. Specify default parameters that apply to all processed tables and a list of tables for which one or more defaults are overridden.



Optim Directory

Specify the ***Optim*** Directory for which audit parameters are defined. If your site has more than one ***Optim*** Directory, click the down arrow to select from a list.

Audit results are stored in the PSTAUDIT table, in the ***Optim*** Directory. If authorized, you may browse or edit the PSTAUDIT table in the same way you browse or edit any other database table. However, **Auditing Status** in Product Options must be set to **Active** or **Active/User** and you must have database SELECT authority for the PSTAUDIT table.

Auditing Defaults

Specify the defaults for the auditing option at your site:

Enabled — Select to audit processing for *all* tables, unless overridden in the Table Name/Pattern list. For example, if a table (or pattern) is listed and **Disabled** status is specified, the table is not audited.

Write All Columns Select to record information for *all* columns in updated, deleted, or inserted rows, unless overridden in the Table Name/Pattern list. If you clear this check box, audit information is recorded for changed columns, inserted rows, and tables that do not have a primary key.

Days to Retain Specify the maximum number of days (0 to 999) to retain Audit information, unless overridden in the Table Name/Pattern list. Audit information is purged automatically after the specified number of days elapse. Specify zero (0) or leave blank to retain Audit information indefinitely.

Maximum Rows Specify the maximum number of audited rows (0 to 999999) to retain for each database table, unless overridden in the Table Name/Pattern list. The oldest rows are deleted to create space to accept new rows. Specify zero (0) or leave blank to retain an unlimited number.

Table Name/Pattern List

Tables for which table-specific audit parameters apply. If you select the **Active/User** option for auditing database tables, the Product Options list supersedes any list users may specify in Personal Options.

Table Name/ Pattern Specify the fully-qualified name of the database table or a pattern that identifies the database tables, in the form *dbalias.creatorid.tablename*. You can also right-click a grid cell and select **Add Tables** to display a selection list.

Status Select the auditing status for the table or tables. Click to display a down arrow and select **Enabled** or **Disabled** for each table or pattern in the list. Use this selection to override the default status established with the **Enabled** check box.

Note: If auditing is disabled for a table, other table-specific parameters cannot be edited.

If a table is listed in both Personal Options and Product Options, the status in Personal Options is **Superseded by Product List**. The user cannot change the auditing status for that table. Users can modify the table name, however, or remove it from the list.

Days to Retain Specify the maximum number of days (1 to 999) to retain audit information for the table or tables. To retain Audit information indefinitely, specify zero (0) or leave blank.

Max Rows Specify the maximum number of audit rows (1 to 999999) retained for each database table or tables. To retain an indefinite number of rows, specify zero (0) or leave blank.

Note: The **Max Rows** limit is checked after 15 commits to the database table.

Write Option Select the level of audit information to record for the table or tables. Click to display a down arrow and select:

- **All Columns** to record audit information for all columns in edited rows.
- **Changed Columns** to record audit information as follows:
  - Record an image of all columns in an inserted row.
  - Record an image of the primary key column in a deleted row. If there is no primary key, record an image of all columns.
  - Record an image of the primary key columns and any changed columns in an updated row.

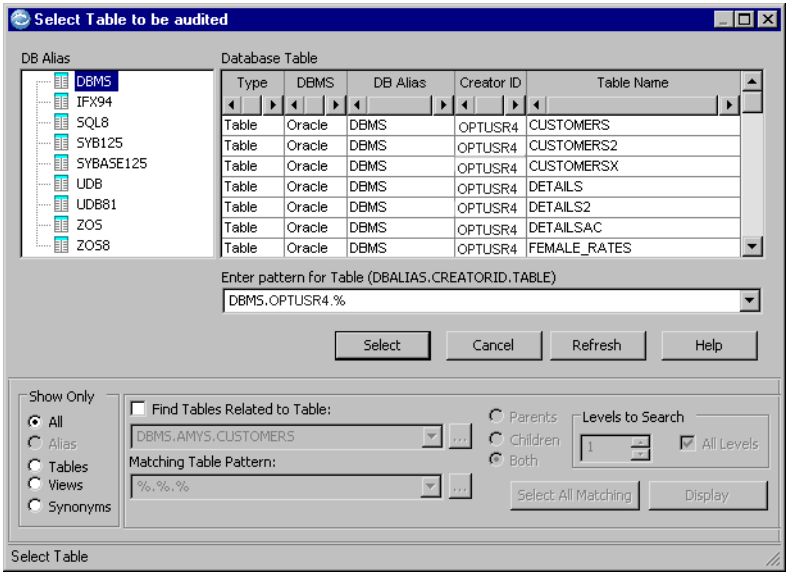
Example

Default specifications are propagated to new entries in the list of tables and can be useful when building the list. For example, if your database includes 100 tables and you want to retain audit information for fifty tables for a period of 90 days, information for thirty tables for a period of 1 year, information for 5 tables for an indefinite period, and do not want to audit processes on the remaining 15 tables, build the list of audit instructions in the following way:

1. Clear **Enabled**.
2. Enter, in the grid, names of the 15 tables that are not audited (select from a list or type names or patterns). **Status** is Disabled for each entry.
3. Select **Enabled** and set **Days to Retain** to 0.
4. Enter, in the grid, names of the five tables for which audit information is retained indefinitely (select from a list or type names or patterns). **Status** is Enabled and **Days to Retain** is 0 for the 5 new entries.
5. Set **Days to Retain** to 365.
6. Enter names of the thirty tables in the grid (select from a list or type names or patterns). **Status** is Enabled and **Days to Retain** is 365 for the 30 new entries.
7. Set **Days to Retain** to 90.
8. The fifty remaining tables are not entered in the grid. The default status for these tables is Enabled and audit information for each table is retained for 90 days.

Select Table To Be Audited Dialog

When you select **Add Tables** or **Replace Table** from the shortcut menu, the **Select Table to be audited** dialog is displayed. This dialog is also displayed when you use the Join command from the Table Editor.



The **Select Table to be audited** dialog provides a list of tables for the selected database.

- DB Aliases for available databases are listed on the left. To list tables in a database, double-click the DB Alias or overtype the DB Alias in the Pattern box.
- Objects referenced by the selected DB Alias are listed in the Database Table grid in alphabetical order by Creator ID and Table Name. The type of object (table, view, alias, synonym), DBMS, and fully-qualified name are provided.

Pattern

Use a pattern to limit the list of objects in the **Select Table to be audited** dialog. After you specify a pattern, click **Refresh** to redisplay the list based on your criteria.

Audit Summary

During an Edit Process, ***Optim*** audits tables according to the following parameters:

If **Active**

Check for the table name on the Product Options list in the **Audit Tables** dialog:

- If the table is on the list and **Enabled**, the table is audited.
- If the table is on the list and **Disabled**, the table is not audited.

If the table is not on the list, and the **Enabled** check box under Auditing Defaults in Product Options is selected, the table is audited.

If **Active/User**

Check for the table name on the Product Options list in the **Audit Tables** dialog:

- If the table is on the list and **Enabled**, the table is audited.
- If the table is on the list and **Disabled**, the table is not audited.

Check the **Edit** tab in the **Personal Options** dialog to determine if the **Auditing Active** check box is selected. If it is, check for the table name on the Personal Options list in the **Audit Tables** dialog:

- If the table is on the list and **Enabled**, the table is audited based on the default specifications in Product Options.
- If the table is on the list and **Disabled**, the table is not audited.

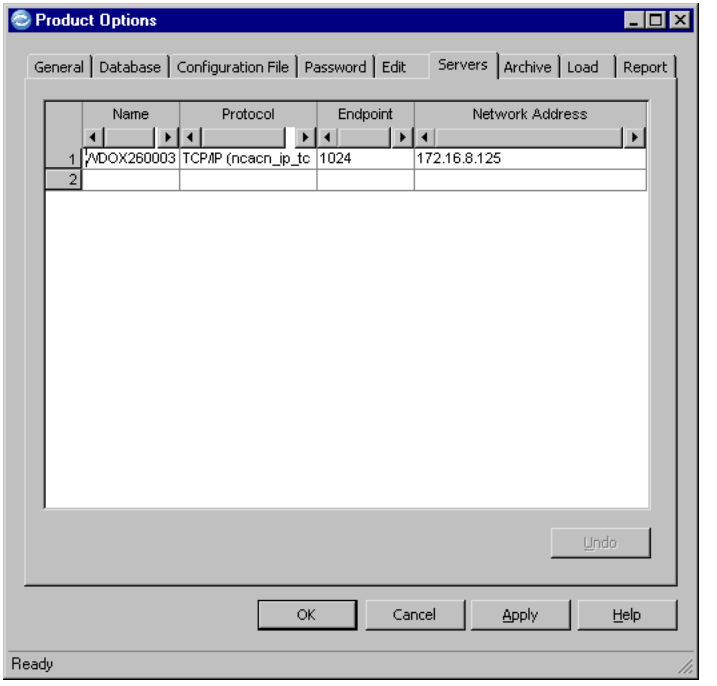
If the table is not on either list, and the **Enabled** check box under Auditing Defaults in Product Options is selected, the table is audited.

If **Inactive**

The audit feature is disabled and the table is not audited.

8.2.6 Servers Tab

When a task requires the movement, processing, or storage of very large volumes of data, the request can be defined at a workstation in the normal way, then directed for remote processing on a machine hosting the ***Server***. If a workstation on your network is configured as a ***Server***, you must provide the appropriate communication protocols so that other workstations can transfer process requests to it. Use the **Servers** tab to specify communication parameters for any ***Servers*** on your network.



Server Name

Enter the name of each ***Server*** (that is, the name given each ***Server*** when it was configured), with the corresponding connection information, as follows.

Supported Protocols (all)

Optim generates endpoints for all possible protocols; client machines connect via RPC Locator Service, where possible.

NetBIOS over TCP (ncacn_nb_tcp)

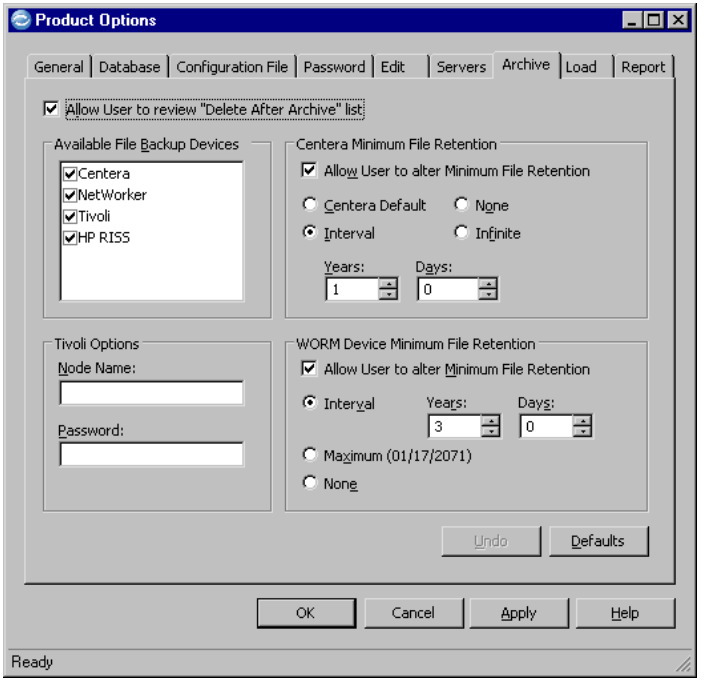
Endpoint: Integer from 1 through 254
Example: 100
Network Address: Windows computer name

NetBIOS over IPX (ncacn_nb_ipx)	Endpoint: Integer from 1 through 254 Example: 100 Network Address: Windows computer name
NetBEUI over NetBIOS (ncacn_nb_nb)	Endpoint: Integer from 1 through 254 Example: 100 Network Address: Windows computer name
TCP/IP (ncacn_ip_tcp)	Endpoint: Internet Port Number Example: 1024 Network Address: Four-octet internet address, or host name
Named Pipe (ncacn_np)	Endpoint: Windows named pipe, starting with "\\pipe" Example: \\pipe\\pipename Network Address: Windows server name
SPX (ncacn_spx)	Endpoint: Integer from 1 through 65535 Example: 5000 Network Address: IPX internet address, or Windows server name
DECnet (ncacn_dnet_nsp)	Endpoint: DECnet phase IV object number, preceded by # character, or object name Example: mailserver #17 Network Address: Area and node syntax
Apple Talk DSP (ncacn_at_dsp)	Endpoint: A character string, up to 22 bytes long Example: myservicesendpoint Network Address: Windows server name, optionally followed by @ and the AppleTalk zone name
Banyan Vines SSP (ncacn_vns_spp)	Endpoint: Vines SPP port number from 250 through 511 Example: 500 Network Address: StreetTalk server name of the form item@group@organization
Internet Information Server (IIS) (ncacn_http)	Endpoint: Internet port number Example: 2215 Network Address: Internet address or local Windows server name

Note: You can specify a dynamic endpoint for any protocol using an asterisk (*). If Supported Protocols (All) is specified, an asterisk (*) displays automatically.

8.2.7 Archive Tab

Use the **Archive** tab to allow users to review data to be deleted after it has been archived, select available backup devices, and set a default minimum file retention period for supported devices.



Allow User to review "Delete After Archive" list

Select this check box to enable the **Review Archive Delete List** check box on the Archive and Delete Request Editors. This check box allows users to display and review the names of tables for which data is to be deleted as a function of archiving.

Available File Backup Devices

Select the appropriate check box(es) to make available one or more backup devices for use with ***Archive***. (The check boxes are cleared by default.)

Centera Select this check box if Centera is available. If you select this check box, the Centera Minimum File Retention box becomes available.

NetWorker Select this check box if EMC NetWorker is available.

Tivoli Select this check box if Tivoli is available. If you select this check box, the Tivoli Options box becomes available.

Note: To use a Tivoli device, you must install the Tivoli client and API support on the machine where the ***Optim Server*** runs.

HP RISS Select this check box if HP RISS is available.

Note: You can copy an Archive File to a backup device by referencing a Storage Profile (with the necessary backup device parameters) in an Archive Request. For details, refer to the ***Archive*** **User Manual,** **Storage Profile**.

Tivoli Options

Node Name Specify an identifier that allows access to the Tivoli tape backup device.

Password Specify a password that allows access to the Tivoli tape backup device.

Centera Minimum File Retention

Specify the default minimum retention period for protecting Archive Files on Centera from deletion. The minimum retention period is measured from the time the Archive Process copies the file to Centera. After the minimum retention period expires, the file can be deleted from Centera.

Allow User to alter Minimum Retention Select this check box to enable the Minimum File Retention setting in the Storage Profile Utility, allowing users to override the default minimum retention defined in Product Options.

Centera Default Select to use the Centera default minimum retention period, based on your Centera configuration.

Infinite Select to keep an Archive File on Centera forever; the file cannot be deleted.

Interval Select to protect an Archive File from deletion for a specified period. You can specify a number of years, days, or a combination of both.

When you select **Interval**, the **Years** and **Days** boxes become available.

Years Specify the number of years (0 to 100) to protect an Archive File from deletion. The default value is zero (0).

Days Specify the number of days (0 to 18300) to protect an Archive File from deletion. The default value is zero (0).

Note: 18300 days equals 50 years.

None Do not use a minimum retention period; allow an Archive File to be deleted from Centera at any time.

WORM Device Minimum File Retention

Specify the default minimum retention period for protecting Archive Files on a WORM device from deletion. The minimum retention period is measured from the time the Archive Process copies the file to the device. After the minimum retention period expires, the file can be deleted from the device.

Allow User to alter Minimum File Retention Select this check box to enable the **WORM Device Minimum File Retention** options in the Storage Profile Utility, allowing users to override the default minimum retention defined in Product Options.

Interval Select to protect an Archive File from deletion for a specified period after the file is generated. You can specify a number of years, days, or a combination of both.

When you select **Interval**, the **Years** and **Days** boxes become available.

Years Specify the number of years to protect an Archive File from deletion. The default value is zero (0).

Days Specify the number of days (0 to 999) to protect an Archive File from deletion. The default value is zero (0).

Note: The interval cannot exceed the maximum date, 01/17/2071. *Archive* checks the interval when you set the Product Options, save a Storage Profile, and run the Archive Process.

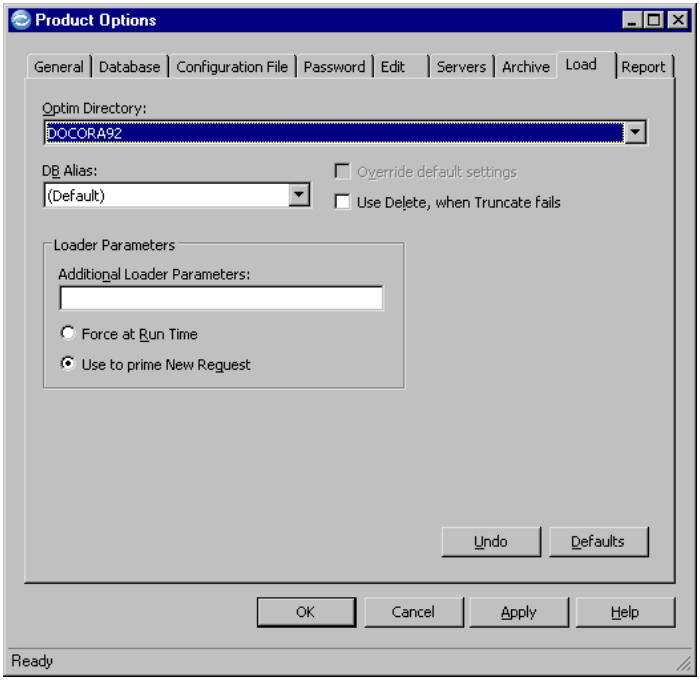
Maximum Use the maximum date, 01/17/2071.

None Do not use a minimum retention period; allow an Archive File to be deleted from the device at any time.

8.2.8 Load Tab

Use the **Load** tab to customize loader parameters and enforce loader requirements for your site. This can be particularly helpful when you have more than one database, or more than one ***Optim*** Directory. You can specify default parameters applicable to all defined DB Aliases, and as needed, specify unique parameters for each different database, each instance or version of a database, or each different ***Optim*** Directory.

For example, after selecting an ***Optim*** Directory, you can select [Default] in the DB Alias box. Loader settings you define will apply to all DB Aliases in the selected ***Optim*** Directory. If the default settings are not appropriate for one DB Alias, you can select that DB Alias in the DB Alias box, select the **Override default settings** check box, and define specific settings for that DB Alias only. You can repeat the procedure for any or all DB Aliases in the selected ***Optim*** Directory, and similarly, for all DB Aliases in each Optim Directory.



Optim Directory

Select the name of the ***Optim*** Directory containing the DB Aliases for which you want to customize loader parameters. If your site has more than one ***Optim*** Directory, and you want to specify loader parameters

for DB Aliases contained in those directories, click the down arrow to select from a list.

DB Alias

Click the down arrow to select from the available DB Aliases in the selected ***Optim*** Directory. If you select [Default], the custom loader parameters you specify apply to all DB Aliases in the selected ***Optim*** Directory.

Override default settings

Select to define unique loader parameters for a specific DB Alias, when default values are defined for all DB Aliases in a selected Optim Directory.

Use Delete, when Truncate fails

This check box is applicable to SQL Server and Sybase ASE DB Aliases only. When **Replace** is specified in a Load Request, data loaded to the affected tables is truncated, unless the particular table is partitioned, in which case the truncate action will fail. Select this check box to issue the SQL Delete statement when the SQL Truncate statement fails.

Note: The SQL Delete statement may be significantly more resource-intensive than the SQL Truncate statement.

Loader Parameters

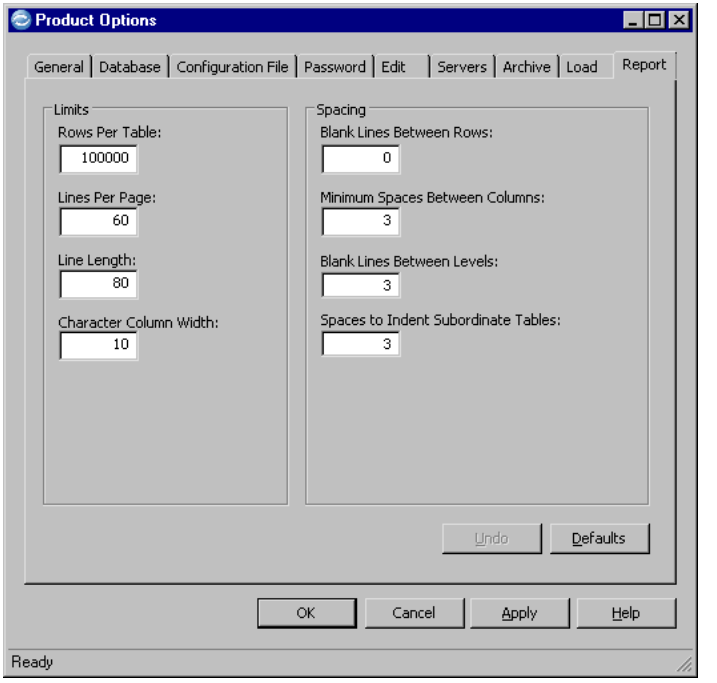
Additional Loader Parameters — Define additional loader parameters, as required, to append to the list created by ***Optim*** for loading data with a DBMS loader. See DBMS documentation for valid operands.

Force at Run Time — Select to force the use of the additional loader parameters defined in Product Options in place of any additional loader parameters specified in a particular Load Request.

Use to prime New Request — Select to populate new Load Requests with the additional loader parameters defined in Product Options. These parameters may be edited in the individual Load Requests, as necessary.

8.2.9 Report Tab

Use the **Report** tab to set formatting defaults for the Report Process.



Limits

Set default limits for the output of the Report Process.

Rows per Table	Specify the maximum number of rows (1 to 99999999) that can be reported on during a single Report Process.
Lines per Page	Specify the maximum number of lines per page (1 to 999) for the report.
Line Length	Specify the maximum number of characters per line (1 to 999) for the report.
Character Column Width	Specify the maximum number of characters per column (1 to 999) for the report.

Spacing

Set default spacing preferences for the output of the Report Process.

Blank Lines Between Rows	Specify the number of blank lines to insert between each row in the report.

Minimum Spaces Between Columns	Specify the number of blank spaces to insert between each column in the report.
Blank Lines Between Levels	Specify the number of blank lines to insert between each level of related tables, when **Show Joins** is enabled, and related tables are joined. (Archive File Report only)
Spaces to Indent Subordinate Tables	Specify the number of blank spaces to indent rows from each subordinate joined table in the report. (Archive File Report only)

9. Personal Options

You can use Personal Options to customize ***Optim*** for use at each workstation. For example, you can:

- Specify default data directories, set user-defined database logon and password information, and select other options to customize display features and message text.
- Provide defaults for the Schedule and Create utilities, and the Load, Edit, and Browse Processes.

Personal Options are recorded in the Windows Registry of the workstation.

Note: Product Option settings (site-level) supersede any conflicting Personal Option settings (user-level). For more information, refer to **Chapter 8. Product Options**.

9.1 Open the Personal Options Editor

You can use the **Configuration** program to configure Personal Options, or you can set options from within ***Optim***.

Using the Configuration program

To configure Personal Options using the Configuration program:

1. Open the **Configuration** program.
2. In the main window, select **Configure Options** from the **Tasks** menu.
3. Specify a PST Directory and click **Proceed**.
4. Click **Skip** on the **Initialize Security/Change Security Administrator**, **Enable/Disable the Optim Server Feature**, and **Enable/Disable the Archive ODBC Feature** dialogs to open the **Specify Product Configuration File** dialog.
5. Select **Create New File** or **Use Existing File**, verify the name of the Configuration File, and click **Proceed**.
6. On the **Modify Product Options** dialog, click **Proceed** to open the **Modify Personal Options** dialog.
7. Click the **Personal Options** button to open the **Personal Options** dialog.
8. Specify the necessary details on each tab in Personal Options.
9. Choose one of the following:
   - To close the **Personal Options** dialog without saving your changes, click **Cancel**.
   - To save your changes and continue using the **Personal Options** dialog, click **Apply**.
   - To save your changes and close the **Personal Options** dialog, click **OK** to return to the **Modify Personal Options** dialog.
10. Click **Proceed** to complete the process.

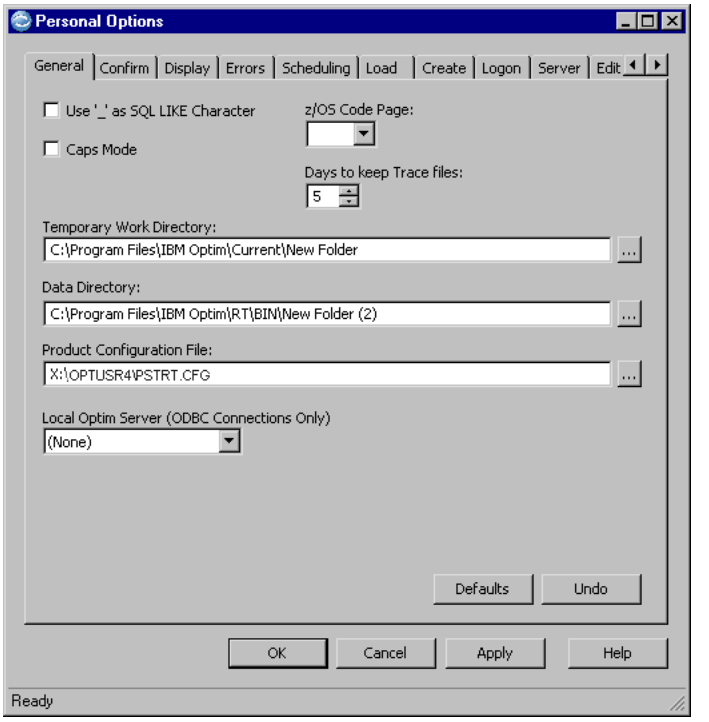
Within *Optim*

To change the settings within Optim:

1. In the main window, select **Personal** from the **Options** menu.
2. On the **Personal Options** dialog, provide the necessary information on each tab.
3. Choose one of the following:
   - To close the **Personal Options** dialog without saving your changes, click **Cancel**.
   - To save your changes and continue using the **Personal Options** dialog, click **Apply**.
   - To save your changes and close the **Personal Options** dialog, click **OK**.

9.2 Using the Editor

The **Personal Options** dialog allows you to customize ***Optim*** for the workstation.



Tabs

The tabs in the **Personal Options** dialog are described briefly in the following paragraphs. Detailed information is provided in each section of this chapter.

General Identify the Temporary Work Directory, Data Directory, and the directory for the Product Configuration File used by the workstation. Options allow you to use the underscore as an SQL LIKE character, select the uppercase or lowercase default for selection criteria, establish the number of days to keep Trace Files, specify a default code page value, and choose whether to warn a user when a cascading delete or update may occur.

Confirm Choose to display a confirmation prompt before definitions are deleted, files overwritten, or DDL lost.

Display	Choose options for data displays when editing data or using Point and Shoot, including the maximum number of rows fetched and the maximum number of entries in history and menu file lists. Also, set options to determine the default settings for Large Objects for the Access Definition.
Errors	Select font characteristics for informational, warning, and error messages and the number of lines to display in the message bar.
Scheduling	Select options for using the Scheduling Monitor.
Load	Provide the complete path and name of the executable used to access each DBMS Loader.
Create	Specify default options for creating database objects.
Logon	Review logon information for each DB Alias in a selected ***Optim*** Directory. Connection and password information is stored in the workstation registry.
Server	Provide User ID, password, and domain information to be used by the ***Optim Server*** (***Server***) when running actions remotely.
Edit	Select options for browsing or editing database tables.
Browse	Select display options for browsing Archive, Extract, Control, or Compare Files. Set defaults for emphasizing differences between rows when browsing Compare Files.
Archive	Identify the default Archive Directory and Archive Index Directory and select options that apply when archiving data.
Removable Media	Provide default segment size values.
Actions	Set options for displaying tabs in Action Request Editors, printing Column Map procedures, and retaining reports.
Printer	Set printer, font, and language preferences for printing a request or definition.

Database Select options for handling multi-byte round trip conversion errors, cascade deletes, and database connections. (For Sybase ASE, you can also specify whether to run in Unchained mode.)

Notify Specify default options and a list of addresses used for sending an email message when a request is processed, or only if a request succeeds or fails.

9.2.1 General Tab

Use the **General** tab to identify the Temporary Work Directory, Data Directory, and the directory for the Product Configuration File used by the workstation, and other defaults.

Use '_' as SQL LIKE Character Select to use the underscore character to represent any single character in a pattern. For example, if **Use '_' as SQL LIKE Character** is selected, you can type PSTDEMO.M _ _ P in the pattern box on the **Open an Access Definition** dialog to list only Access Definitions with a name beginning with M and ending with P for the Identifier PSTDEMO. If you clear this check box, the underscore represents the underscore character.

Caps Mode Select to convert all lowercase characters to uppercase when you specify string literals in selection criteria, relationships, and Column Maps. If you clear this check box, characters display in uppercase or lowercase, exactly as entered.

z/OS Code Page In an ***Optim*** process, you can use an Extract File created using the ***Optim*** **z/OS Solution**. ***Optim*** uses a code page to convert the mainframe file format from EBCDIC to ASCII. In the **z/OS Code Page** list, select a default value to be used if the Extract File does not contain a code page number.

Days to keep Trace files Specify the number of days (2 to 30) to retain trace files in the temporary work directory. The default value is 5.

Trace files are useful for ***Optim*** to track processing. Trace file names are prefixed with PR0, followed by letters indicating the trace file type, and ended with a numeric extension (for example, PR0TOOL.123). The extension on the name of the trace file distinguishes one trace file from another of that type. Trace files are sequentially numbered .001 through .999, followed by .A00 through .Z99, as necessary. If more than 3,599 trace files of a single type are created and stored within the specified number of days, file names are reused, beginning with the first.

Note: Storage space limitations should be considered when deciding the number of days to retain the files.

Temporary Work Directory

Specify the complete path to the default directory in which you want to store internal work files and trace files. To select from your system directories, click the browse button.

Data Directory

Specify the complete path to the default directory in which you want to store Archive, Extract, Control, Compare, and Export Files, and other process files. To select from your system directories, click the browse button. The Data Directory serves as the default; you can specify a different directory path and file name on any process request.

Product Configuration File

Specify the complete path to the Product Configuration File. The file name has a **.cfg** extension. To select from your system directories, click the browse button. The Product Configuration File is created when you install ***Optim***.

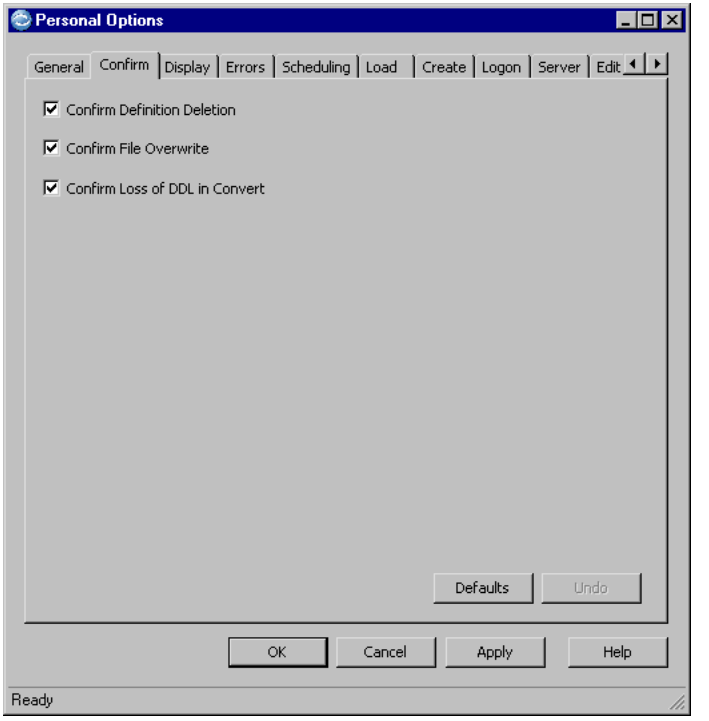
Local Optim Server (ODBC Connections Only)

To improve ODBC response times, select the name of the ***Server*** that runs on this machine. The ***ODBC Server*** will run locally and the ***Server*** will not be contacted, if an ODBC connection specifies this ***Server*** name, or if the ODBC interface selects an Archive File with this ***Server*** name in its Archive Directory entry.

Note: Do not use this setting if accessing archived data on a backup device.

9.2.2 Confirm Tab

Use the **Confirm** tab to choose whether a confirmation dialog is displayed before the execution of a process that results in loss of data.



Confirm Definition Deletion

Select to display a confirmation dialog before you delete a definition or process request from the ***Optim*** Directory. Selecting this check box helps prevent deleting a request or definition accidentally.

Confirm File Overwrite

Select to display a confirmation dialog before you overwrite an existing file (Archive File, Extract File, Control File, Compare File, or Export File).

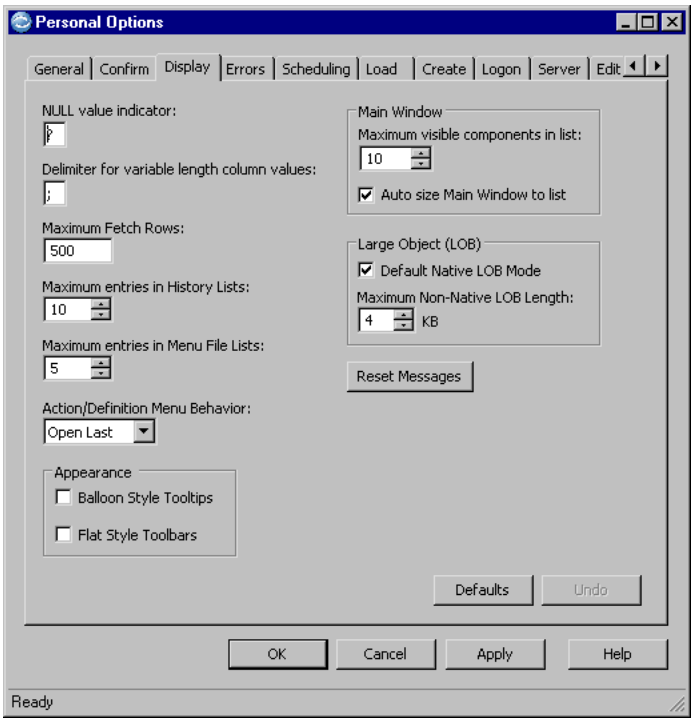
Note: If you select this check box, a confirmation dialog opens before you run a process. However, this confirmation does not display for a process request that is scheduled or run using the Command Line Interface.

Confirm Loss of DDL in Convert

Select to display a confirmation dialog during a Convert Process that can result in the loss of DDL statements. The confirmation dialog is not displayed for a scheduled process request.

9.2.3 Display Tab

Use the **Display** tab to select preferences for displaying information.



NULL value indicator

Enter a character to represent a NULL value. The question mark (?) is the default. Although you can choose any character to represent a NULL value, an infrequently used character is best.

Delimiter for variable length column values

Enter a character to delimit variable length column values that have trailing blanks. The semi-colon (;) is the default. Although you can choose any character as a delimiter, an infrequently used character that differs from the NULL value indicator is best.

Maximum Fetch Rows

Specify the maximum number of rows from a single table that can be displayed when you browse or edit table data or use Point and Shoot. You can enter a number from 1 through the site maximum, specified on the **Product Options** dialog. The default value is 500.

Maximum entries in History Lists

Specify the maximum number of recently selected items (1 to 20) displayed in a drop-down list. For example, the Extract File box in a request editor, where you can click the down arrow to view a list of the most recently used Extract Files.

Maximum entries in Menu File Lists

Specify the maximum number of items (1 to 20) displayed below the **File** menu commands in an editor. For example, a list of the most recently opened definitions appears on the **File** menu in the Access Definition Editor.

Action/Definition Menu Behavior

Click the down arrow to select the default mode for opening the action or definition editors from the **Actions** or **Definitions** menu in the main window.

Open Last	Opens the last edited request in the selected editor. This is the default.
Open New	Opens a new, untitled request in the selected editor.

Appearance

Options for displaying tooltips and toolbars on dialogs and editors in ***Optim***.

Balloon Style Tooltips	Controls the appearance of the tooltips. Select the check box to choose balloon-style. Clear the check box to choose flat-style (default).
Flat Style Toolbars	Controls the appearance of the toolbars. Select the check box to choose flat-style. Clear the check box to choose 3D style (default).

Main Window

Options for displaying the list of active dialogs and editors in the main window. As you open each editor or dialog, the main window expands to list the active editors and dialogs. To recall an active editor or dialog, double-click the item in the list.

Maximum visible components in list	Specify the maximum number of active editors or dialogs (5 to 99) displayed in the main window. The default value is 10. If the number of active editors and dialogs exceeds the maximum, you can scroll the list. (If fewer editors or dialogs are in use, the bottom of the list is blank.)
Auto size Main Window to list	Select to automatically resize the main window as editors and dialogs are added to the list. If you clear this check box, the main window is sized to display the maximum number of editors and dialogs that can be listed.

Large Object (LOB)

Default Native LOB Mode

Select this check box to set the default for the **Native LOB Mode** check box on the **Columns** tab of the **Table Specifications** dialog, available through the Access Definition Editor. You can use the check box on the **Table Specifications** dialog when preparing an Access Definition for use with ***Edit***. When editing, the check box designates whether to start the native application associated with an LOB, or to process as a VarChar or VarBinary data type.

Maximum Non-Native LOB Length

Specify the maximum length of data to retrieve from a database for an LOB processed as a VarChar or VarBinary data type when using the Table Editor in ***Edit***. Select a value from 1 KB through 32 KB.

Note: The setting of the **Native LOB Mode** check box on the **Columns** tab of the **Table Specifications** dialog (available through the Access Definition Editor) determines whether an LOB is processed as Native or Non-Native.

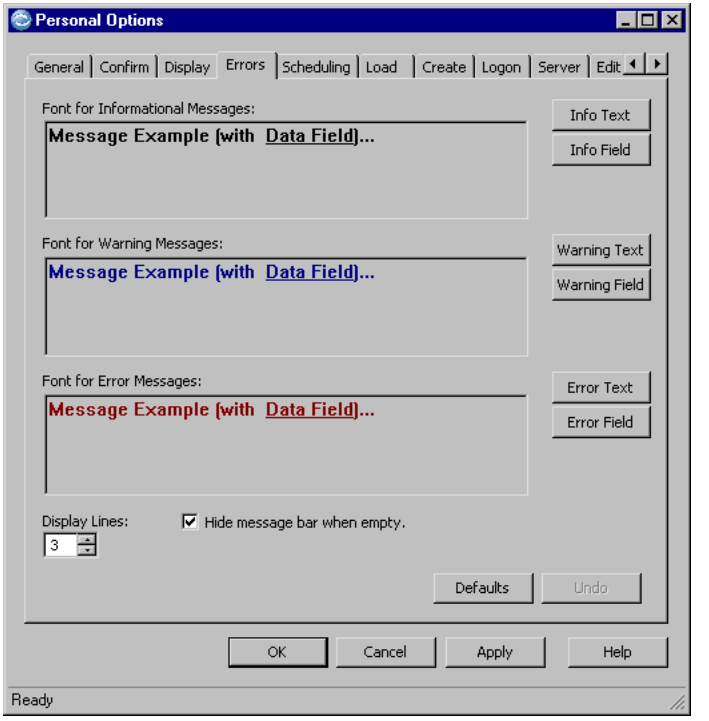
An LOB truncates when the size of the LOB exceeds the Maximum Non-Native LOB Length setting, and appears in the Table Editor as a protected cell with a cross-hatched pattern.

Reset Messages

Click **Reset Messages** to reset system messages. Message dialogs provide information or warnings. You can also choose *not* to display the message again. **Reset Messages** resets the option to display these message dialogs, when appropriate.

9.2.4 Errors Tab

Use the options on the **Errors** tab to set preferences for the display of error messages.



The default fonts for message text and data fields are shown in each of the font message boxes. To open the Windows **Font** dialog to select font attributes, click the command buttons for text or fields. To modify the font for text messages, click **Text**. To modify the font for data fields noted in message text, click **Field**.

Font for Informational Messages

Informational messages are not critical; for example, messages that ask whether information should be saved when a dialog is closed.

Info Text — Specify font characteristics for the informational message text. The default is System, 10 point, Bold, Black.

Info Field — Specify font characteristics for the data referenced in an informational message. The default is System, 10 point, Bold, Underline, Maroon.

Font for Warning Messages

Warning messages indicate serious, but not critical conditions. A warning message does not interrupt an action, but may indicate that you should reevaluate the current action.

Warning Text Specify font characteristics for the warning message text. The default is System, 10 point, Bold, Maroon.

Warning Field Specify font characteristics for the data referenced in a warning message. The default is System, 10 point, Bold, Underline, Maroon.

Font for Error Messages

Error messages indicate critical conditions and interrupt the current action. A problem presented in an error message must be addressed before the attempted action can proceed. Error messages can appear in pop-up dialogs, but usually display in the message bar at the bottom of a dialog.

Error Text Specify font characteristics for the error message text. The default is System, 10 point, Bold, Navy.

Error Field Specify font characteristics for the data referenced in an error message. The default is System, 10 point, Bold, Underline, Navy.

Display Lines

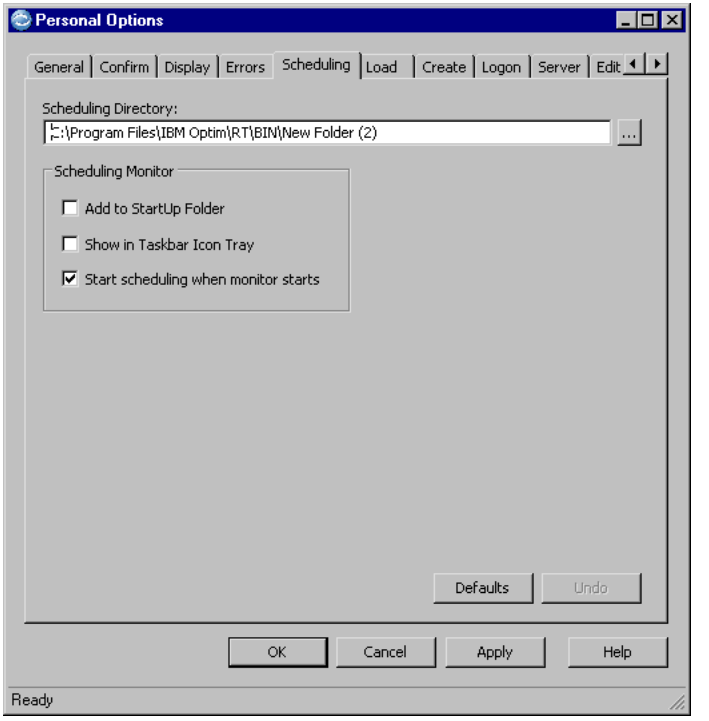
Specify the maximum number of lines (3 to 9) to display in the message bar for any type of message.

Hide message bar when empty

Select this check box to hide the message bar when there are no informational, warning, or error messages to display. If you clear this check box, the message bar appears at the bottom of each editor or dialog at all times.

9.2.5 Scheduling Tab

Use the options on the **Scheduling** tab to specify a default directory for ***Optim*** to store process requests, and to set options for the **Scheduler**.



Scheduling Directory

Enter the full path to the default directory for schedule files. To select from your system directories, click the browse button. Each user should have a unique directory for schedule files.

Scheduling Monitor

Select options for using the Scheduling Monitor. The Scheduling Monitor must be active for scheduled jobs to be processed.

Add to StartUp Folder

Select this check box to add the **Scheduler** to the group of programs that start automatically when you start Microsoft Windows.

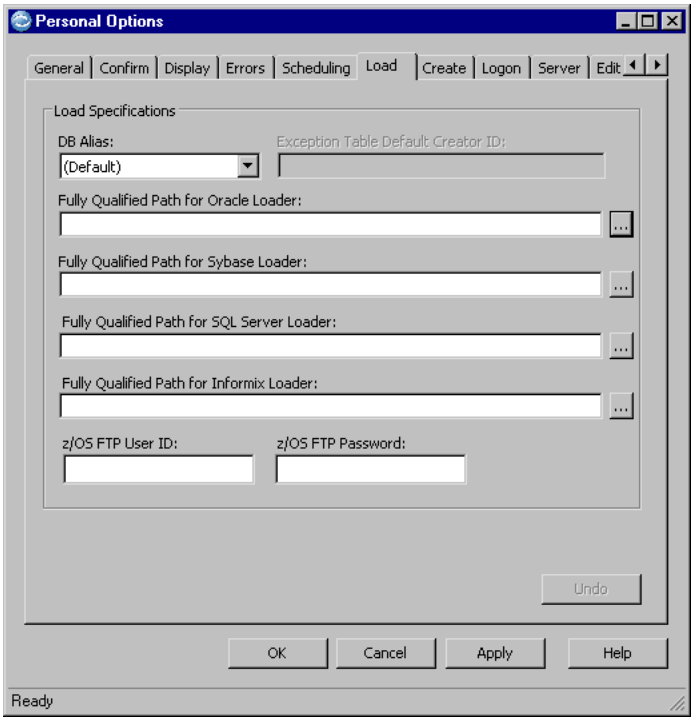
Show in Taskbar Icon Tray

Select this check box to display the **Scheduler** icon in the Microsoft Windows task bar icon tray, instead of as a button on the taskbar.

Start scheduling when monitor starts Clear this check box to prevent starting scheduled jobs immediately when the Schedule Monitor starts.

9.2.6 Load Tab

Use the options on the **Load** tab to set specifications for a Load Process.



Load Specifications Specify the complete path and name of the executable to access each DBMS Loader that can be used with a Load Request.

DB Alias Select [Default] to enter the path and name of the Loader executable file for each DBMS type.

If you have more than one version of a particular DBMS type, you can enter the unique loader specification for each version. Click the down arrow to select the specific DB Alias, then enter the appropriate path and name of the Loader executable file for the particular DBMS version.

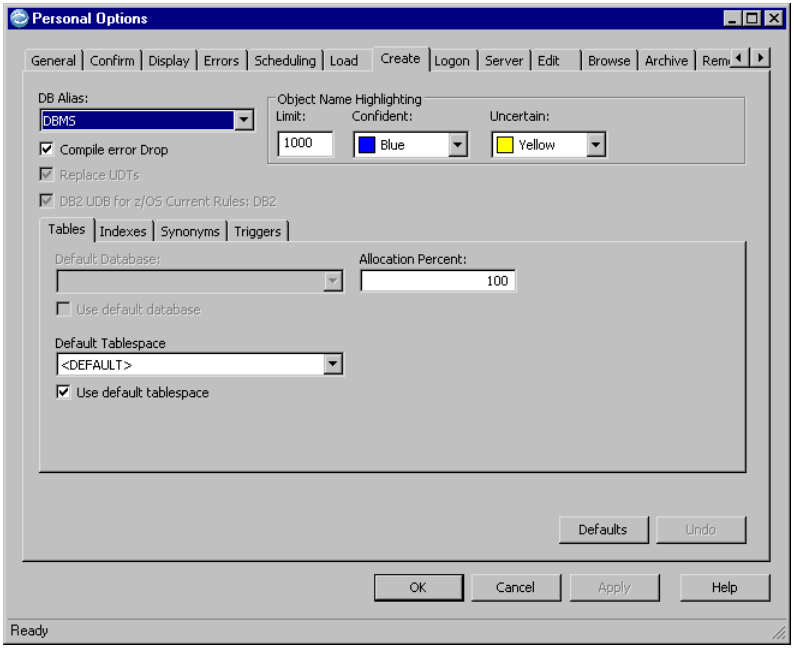
Exception Table Default Creator ID	Specify a default Creator ID for exception tables (DB2 and Oracle) or violation tables (Informix). This field is available only when you select a DB Alias for a DB2, Oracle, or Informix database.
Fully Qualified Path for *DBMS Loader*	Specify the directory path and program name for the specific DBMS Loader. Consult your DBMS documentation for the name of the loader program. To select from your system directories, click the browse button.
z/OS FTP User ID	Provide the default user ID for the z/OS FTP server, used when uploading files to the z/OS machine during the Load Process. This option is available when you select the (Default) or a DB2 **DB Alias**. You can override the user ID in the Load Request.
z/OS FTP Password	Provide the password for the default z/OS FTP server user ID. This option is available when you select the (Default) or a DB2 **DB Alias**. You can override the password in the Load Request.

9.2.7 Create Tab

Use the options on the **Create** tab to set defaults for creating objects. Note that you can establish as many as three layers of default settings for the creation of database objects, in addition to target system defaults. The default settings determine the values displayed in the Object List for the Create Utility and can be overridden at the object level by editing the list.

At the broadest level, DB Alias settings establish defaults for creating objects in the associated database. If desired, you can provide Personal Options settings, as described in the following text, for a user or group of users that override some or all DB Alias settings. A third level of optional defaults apply at the processing level to override Personal

Options and DB Alias settings. Use the options on the **Create** tab to set second-level defaults for the Create Utility.



DB Alias

Specify the DB Alias that identifies the database in which you want to create database objects. To select from a list, click the down arrow. Specify default options for creating different types of database objects on each corresponding tab.

Compile error Drop

Select this check box to automatically drop any Oracle object that causes a compile-type error during the Create Process. If you clear this check box and compile-type errors occur, you must interrupt the Create Process to drop the object before continuing.

This feature applies to Oracle compile-type errors that may occur on certain database objects: functions, packages, package bodies, procedures, triggers, and views. (The Create Process can create these objects, but they may not be functional.) Select this check box to correct possible problems in the **Review SQL** dialog before performing the Create Process.

Replace UDTs

Select this check box to replace table-type column references to User Defined [data] Types with base column data types in any generated DDL. When you clear this check box, references to UDTs are preserved

in generated DDL. (This check box is available only when you select a DB Alias for a DB2, Sybase ASE, or SQL Server database.)

Note: Clear this check box if you want UDT references in the generated DDL.

DB2 OS/390 Current Rules: DB2

Select this check box to require the user (i.e., Create and DDL) to create and delete LOB tablespaces, AUX tables, and unique Indexes. When you clear this check box, DB2 OS/390 automatically creates and deletes LOB tablespaces, AUX tables, and unique Indexes. This check box is selected by default.

Object Name Highlighting

Select a font color to highlight object name changes in the SQL statements shown on the **Review SQL** dialog before creating those objects in the target database. During the Create Process, object names (specified in the Table Map) are translated to be appropriate for the target database. This feature applies to creating text type database objects: functions, packages, package bodies, procedures, triggers, and views.

Limit When creating a large number of objects, highlighting object names in color can affect the speed of the process. Specify the maximum number of created objects to highlight in color (i.e., if the number of objects to create exceeds the limit you specify, colorization is not used). The default is 1000.

Confident Select a font color to highlight object name changes that are reasonably confident. Accept the default color (blue) or click the down arrow to select a different color.

Uncertain Select a font color to highlight object name changes that may require verification because of the way different DBMSs use object names. Accept the default color (yellow) or click the down arrow to select a different color.

Create — Tables Tab

Use the **Tables** tab to specify the default database (for DB2 z/OS). Specify a default tablespace (segment, filegroup, or dbspace) for creating database objects. Specify an allocation percent to adjust SQL storage related parameters (for Oracle and DB2 z/OS).

Default Database

Enter the name of the default database for creating tables. To select from a list, click the down arrow. This option is available only if you are using DB2 z/OS. A single DB Alias in ***Optim*** can identify more than one database in DB2 z/OS.

Use default database

Select this check box to use the default database for creating tables. If you clear this check box, the Create Utility attempts to use the source database from the Source File. However, if the source database does not exist on the target system, the Create Utility uses the default database.

Default...

Enter the name of the default tablespace (segment, filegroup, or dbspace) for creating tables. To select from a list, click the down arrow. If you select <Default>, the default set in the database is used.

Use default tablespace

Select this check box to use the default tablespace (segment, filegroup, or dbspace) for creating tables. If you clear this check box, the Create Utility attempts to use the tablespace (segment, filegroup, or dbspace) in the Source File. However, if the source does not exist on the target system, the Create Utility uses the default.

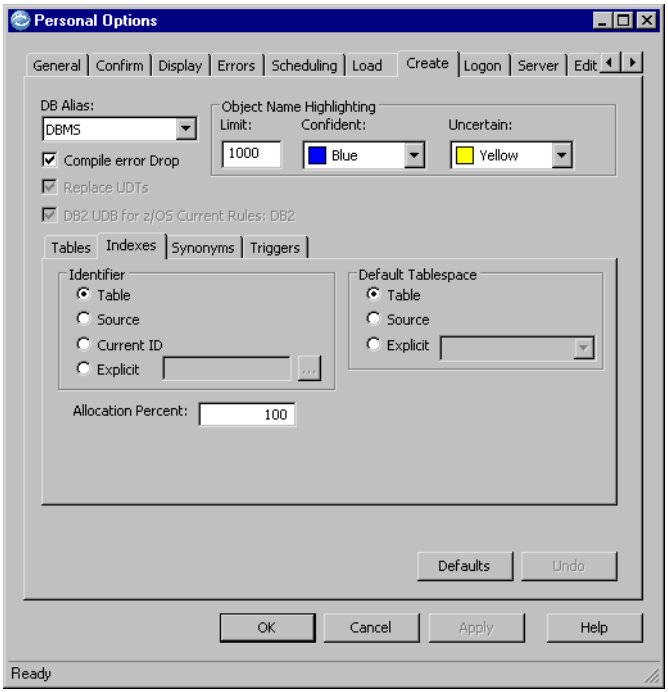
Allocation Percent

Enter a percent (0 to 999) to adjust SQL storage-related parameters for the Create Utility. The default is 100. Allocation percent is available for creating tables and indexes in Oracle and creating indexes in DB2 z/OS.

Target SQL is generated based on the values of the objects in a Source File. If you specify zero (0), the storage-related clause in the SQL statement is omitted. Using any value, other than zero, results in a percentage of the source value being used in the target clause.

Create — Indexes Tab

Use the **Indexes** tab to select a default identifier for creating new indexes. Specify an allocation percent to adjust SQL storage-related parameters (for Oracle and DB2 z/OS). Specify the default tablespace (segment, filegroup, or dbspace) for creating indexes.



Identifier

Specify the default identifier for new indexes based on the identifier from one of the following:

Table Use the identifier from a corresponding target table as the default for new indexes.

Source Use the identifier from the source index as the default for new indexes.

Current ID Use the current SQLID (User ID) as the default for new indexes.

Explicit Use an explicit identifier as the default for new indexes. If you select this option, you must specify an explicit identifier (1 to 64 characters). To select from a list, click the browse button.

Allocation Percent

Enter a percent (0 to 999) to adjust SQL storage-related parameters for the Create Utility. The default is 100. Allocation percent is available for creating tables and indexes in Oracle and creating indexes in DB2 z/OS.

Target SQL is generated based on the values of the objects in a Source File. If you specify zero (0), the storage-related clause in the SQL statement is omitted. Using any value, other than zero, results in a percentage of the source value being used in the target clause.

Default . . .

Specify a default tablespace (segment, filegroup, or dbspace) for creating new indexes, based on one of the following:

Table	Create an index in the same tablespace (segment, filegroup, or dbspace) as the owning table.
Source	Create an index in the same tablespace (segment, filegroup, or dbspace) as the index referenced in the Source File.
Explicit	Create an index in a particular tablespace (segment, filegroup, or dbspace). If you select this option, you must specify the appropriate default. If you select <Default>, the default set in the database is used.

Buffer Pool

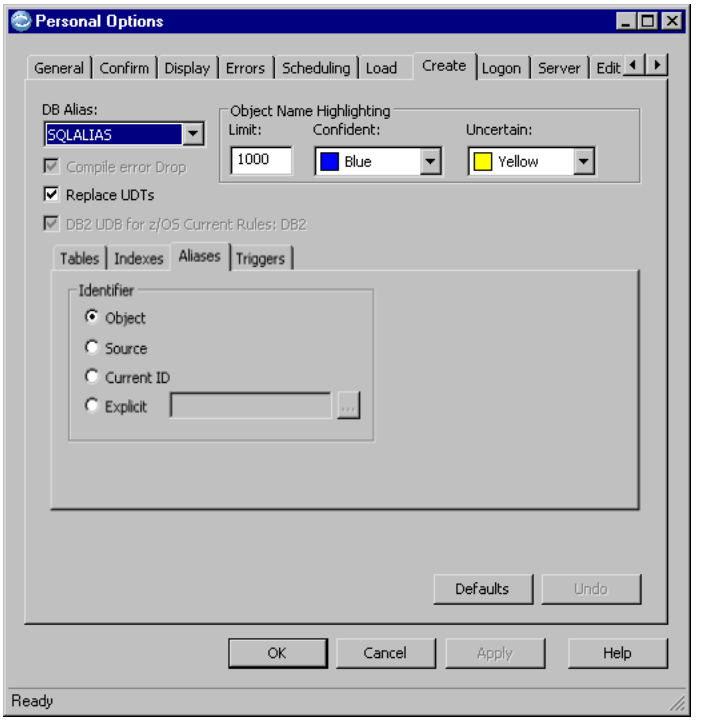
The buffer pool (e.g., BP1) that is to be used when creating an Index. You can enter a specific value for the buffer pool or select a value from the list. (**Buffer Pool** is displayed only for DB2 z/OS.)

The list displays any index buffer pools already specified for this DB Alias (i.e., on the **Index Defaults** tab of the DB Alias Editor), as well as the following:

<DEFAULT>	Select to use the default buffer pool specified by DB2 z/OS. When creating an index, ***Optim*** does not generate a BUFFERPOOL clause in the Create statement.
<SOURCE>	Select to use the same buffer pool as the index for the source Archive or Extract File.

Create — Aliases Tab

Use the **Aliases** tab to select default options for creating new aliases. You can specify a default alias when you use DB2 LUW or DB2 z/OS.



Identifier

Specify the default identifier for new aliases based on the identifier from one of the following:

Object Use the identifier from the corresponding target object as the default for new aliases. For aliases, the corresponding target object is the table, view, or alias referenced in the alias.

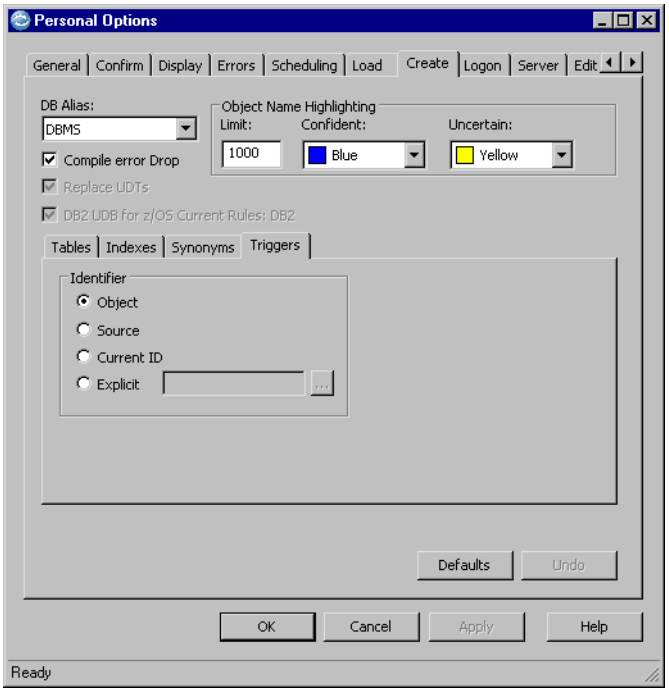
Source Use the identifier from the source alias as the default for new aliases.

Current ID Use the current SQLID (User ID) as the default for new aliases.

Explicit Use an explicit identifier as the default for new aliases. If you select this option, you must specify an explicit identifier (1 to 64 characters). To select from a list, click the browse button.

Create — Triggers Tab

Use the **Triggers** tab to select default options for creating new triggers. You can specify a default trigger when you use DB2 LUW, Oracle, Sybase ASE, SQL Server, or Informix.



Identifier Specify the default identifier for new triggers based on the identifier from one of the following:

Object Use the identifier from a corresponding target object as the default for new triggers. For triggers, the corresponding target object is the table referenced in the trigger.

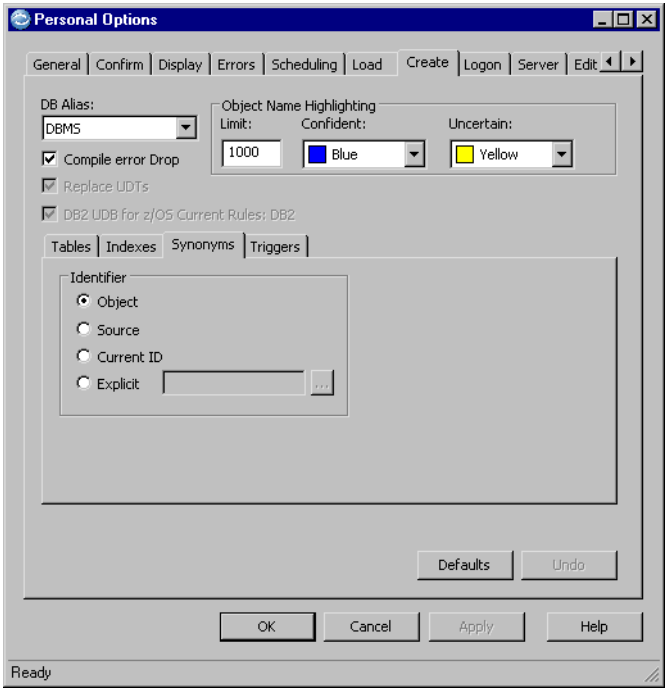
Source Use the identifier from the source trigger as the default for new triggers.

Current ID Use the current SQLID (User ID) as the default for new triggers.

Explicit Use an explicit identifier as the default for new triggers. If you select this option, you must specify an explicit identifier (1 to 64 characters). To select from a list, click the browse button.

Create — Synonyms Tab

Use the **Synonyms** tab to select default options for creating new synonyms. You can specify a default synonym when you use Oracle or Informix.



Identifier

Specify the default identifier for new synonyms based on the identifier from one of the following:

Object Use the identifier from a corresponding target object as the default for new synonyms. For synonyms, the corresponding target object is the table, synonym, function, package, package body, procedure, sequence, trigger, or view referenced in the synonym.

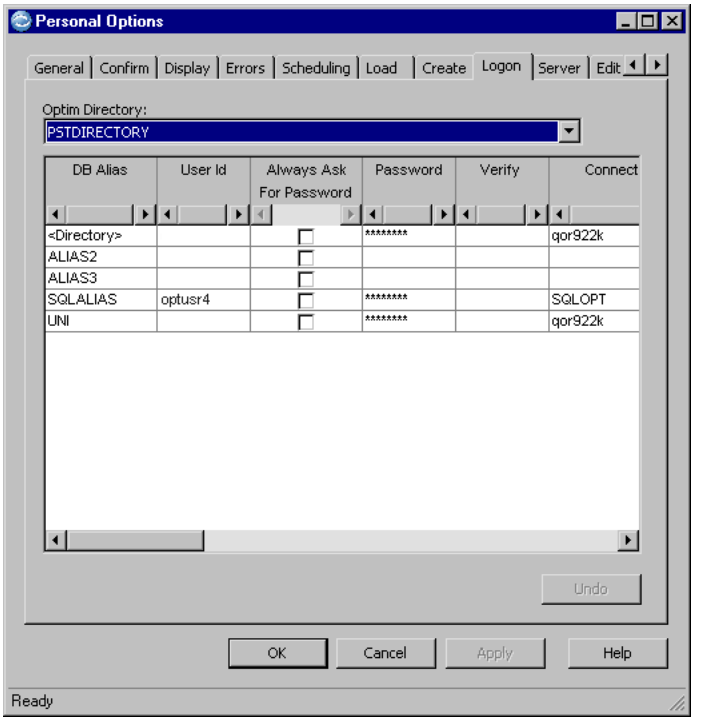
Source Use the identifier from the source synonym as the default for new synonyms.

Current ID Use the current SQLID (User ID) as the default for new synonyms.

Explicit Use an explicit identifier as the default for new synonyms. If you select this option, you must specify an explicit identifier (1 to 64 characters). To select from a list, click the browse button.

9.2.8 Logon Tab

Use the options on the **Logon** tab to set logon and password preferences.



Optim Directory

Select the name of the ***Optim*** Directory to display the corresponding logon information. If you have access to more than one ***Optim*** Directory, click to select from a list.

Grid Details

The logon information corresponding to the selected ***Optim*** Directory includes the following details:

DB Alias List of DB Alias names you can access.

User ID Identifier (1 to 30 characters) that allows you to access a particular DB Alias. User IDs are usually assigned and maintained by the database administrator.

Note: If you are using Informix, you must specify the User ID in uppercase for an ANSI database and in lowercase for a non-ANSI database.

Always Ask For Password	Select to display the logon dialog every time you access a different ***Optim*** Directory or DB Alias. If selected, the **Password** and **Verify** entries are not required. If you clear the check box, the logon dialog appears the first time you access a different ***Optim*** Directory or DB Alias. After you provide a password for an ***Optim*** Directory or DB Alias, it is not necessary to provide a password again. (This check box also appears on the **Logon** dialog.)
Password	Enter a password (1 to 30 characters) that allows you to access a particular database using the specified DB Alias. For security reasons, your password displays as a series of asterisks (****). For versions of DB2 earlier than 6.1, passwords are limited to 8 characters.
Verify	Enter the password again for verification. For security reasons, your password displays as a series of asterisks (****).
Connection String	Connection string used by ***Optim*** to access a particular database using the specified DB Alias.
Always Fail Connection	Select to automatically cancel the logon prompt for a DB Alias that you are not authorized to access or that you choose not to access. If you clear this check box, a logon dialog displays any time you do not have immediate access to a particular DB Alias. (You cannot modify the check box associated with the ***Optim*** Directory.)
Description	Text that describes the purpose of the logon record.

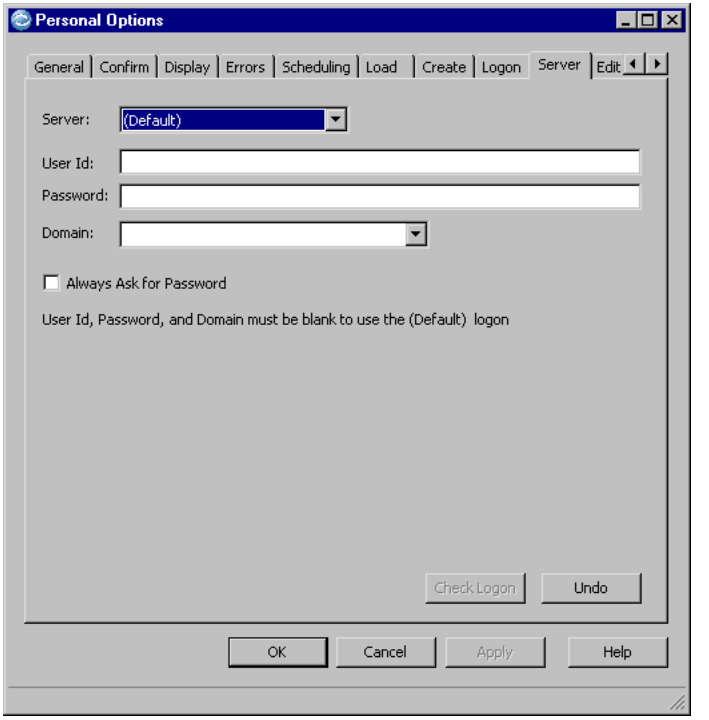
Test the Connection

You can test the DB Alias connection to verify the validity of the DB Alias logon information. To perform the test, right-click in a grid cell and select **Test Connection** from the shortcut menu. A message displays in the Status bar at the bottom of the dialog indicating the success or failure of the test. If you selected the **Always Ask For Password** check box, you are prompted to enter the password.

9.2.9 Server Tab

Use the **Server** tab to provide credentials that may be used when the optional ***Server*** is enabled and tasks are delegated to the ***Server***. The

Server can be configured to use these credentials for access to the ***Optim*** Directory, certain DB Aliases, or the working files.



Server — Select the name of the ***Server*** for which to enter User ID, Password, and Domain information. Click the down arrow to select from the list of ***Servers*** configured in Product Options, or select [Default] to use the same information for all ***Servers***.

User ID — Enter the User ID used by the ***Server*** when performing tasks.

Note: The User ID must have SeBatchLogonRight privileges, or be a member of a "well-known group" with the appropriate authority. This privilege must be granted at the local level for each ***Server*** machine.

Password — Enter the password corresponding to the specified User ID.

Domain — Enter the Domain name used to run actions remotely, or for remote input/output files.

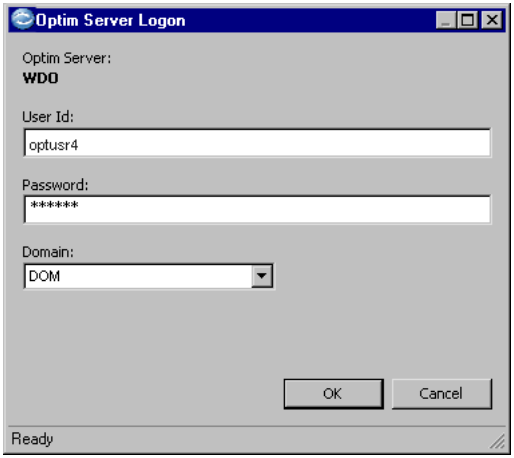
Always Ask for Password — Select to display the **Server Logon** dialog whenever the ***Server*** is used for remote processing calls. When selected, **Password** is not available.

Check Logon

Click **Check Logon** to verify that the ***Server*** can log on with the information provided.

Optim Server Logon Dialog

If you select the **Always Ask for Password** check box, or if the default logon information is incorrect, the **Optim Server Logon** dialog is displayed.



Always Ask for Password

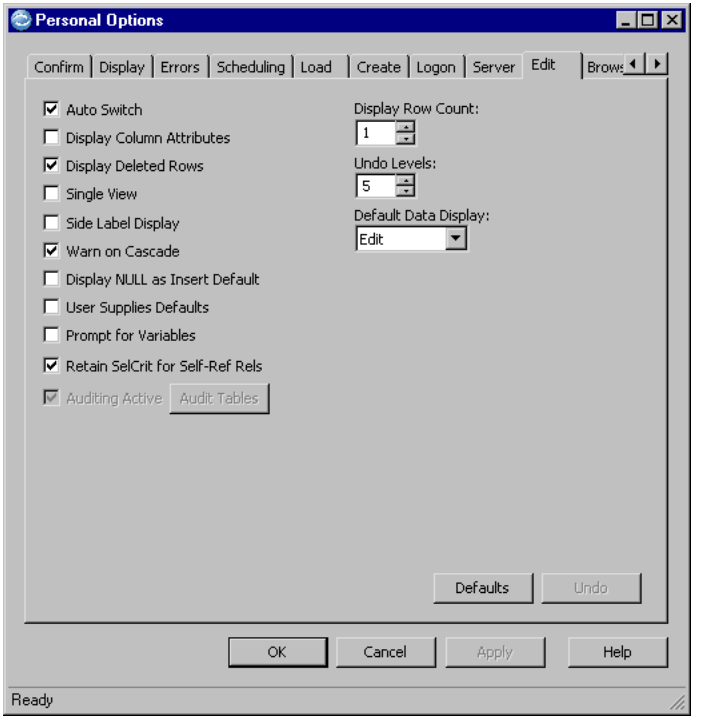
Select to display the **Optim Server Logon** dialog whenever the ***Server*** is used for remote processing calls.

Save as Default Logon

If you select the **Save as Default Logon** check box, the information you enter in this dialog overrides the default settings specified on the **Server** tab in Personal Options.

9.2.10 Edit Tab

Use the options on the **Edit** tab to set preferences for browsing and editing data.



Auto Switch

Select to automatically switch subordinate tables in a stack of two or more joined tables to display related rows.

When you select a row in a table and no related rows exist in the subordinate table, ***Optim*** automatically switches to display the next table in the stack that has a related row.

Display Column Attributes

Select to display column attributes (data type, length, and nullable attribute) for all columns in a selected table. Column attributes are useful when you insert a row or modify column data in the Table Editor.

Display Deleted Rows

Select to display rows that you delete (in Deleted status) in the Table Editor. Deleted rows appear dimmed. To hide deleted rows, clear this check box.

Single View

Select to disable the Join capability when the first item in the Table Editor is a view. Browsing and editing is more efficient using single

view mode because relationship information is bypassed. However, to browse or edit related data, you must clear the check box.

Side Label Display

Select to show column names and values side by side for a single row. To show column names and values for multiple rows (Columnar Display), clear this check box.

Warn on Cascade

Select to display a warning that rows in other tables may be deleted, or column values set to NULL, when you delete rows in a table. The **Delete Confirmation** dialog displays the names of affected tables, including tables that are not shown in the Table Editor. Column values may be set to NULL if the relationship between the tables is using the SET NULL delete rule.

Note: Be certain you want to disable this feature before clearing this check box.

Display NULL as Insert Default

Select to specify NULL as the default value for nullable columns when you insert a new row. If you clear this check box, ***Optim*** provides a value based on the column data type. Other than NULL, possible values include blank, zero, current date, current time, and current timestamp. To specify the character for the NULL value indicator, use the **Display** tab on the **Personal Options** dialog.

Note: Site management may set Product Options to restrict the use of this feature.

User Supplies Defaults

Select to require a user-supplied value for every column that cannot accept a default value. If you clear this check box, ***Optim*** provides a value based on the column data type. Possible values include blank, zero, current date, current time, or current timestamp.

Note: Site management may set Product Options to restrict use of this feature.

Prompt for Variables

Select to request a prompt for default values associated with substitution variables in an Access Definition. You can use substitution variables in selection criteria to specify data to browse or edit.

Retain SelCrit for Self-Ref Rels

Select to apply selection criteria each time a table is self-referenced in the Table Editor. Clear the check box to remove, as the default, selection criteria when the table is self-referenced.

Note: A table can only be self-referenced when the Table Editor is in Browse mode.

Auditing Active

Select to activate the Audit option for tracking database changes when you edit data. If you select this option, click **Audit Tables** to specify the tables you want to audit. If you prefer not to use this option, clear the check box.

Note: Site management may set Product Options to restrict the use of this option.

Audit Tables

Click to open the **Audit Tables** dialog on which you can specify a list of tables to audit.

Note: Auditing is available in Personal Options only if the **Auditing Status** in Product Options is set to **Active/User**.

Display Row Count

Specify the default number of rows to display for each joined table in the Table Editor. Use row count to manage the display area when you join several tables in the Table Editor.

Undo Levels

Specify the default number of times (1 to 20) you can undo a commit to any row in the Table Editor. You can specify the maximum number of undo levels (or commit points) per row.

Use undo commands to restore data in the Table Editor to a prior commit point. For example, if you change three columns in a row and commit that row, you can undo the changes using one undo level. If you set **Undo Levels** to 5 and you commit 7 times on a particular row, you can undo only the last 5 committed changes to that row or return to the original row.

Default Data Display

Select the default mode for adding tables to the Table Editor. Click the down arrow to select **Browse**, **Browse Only**, or **Edit** mode for each table opened or joined in the Table Editor.

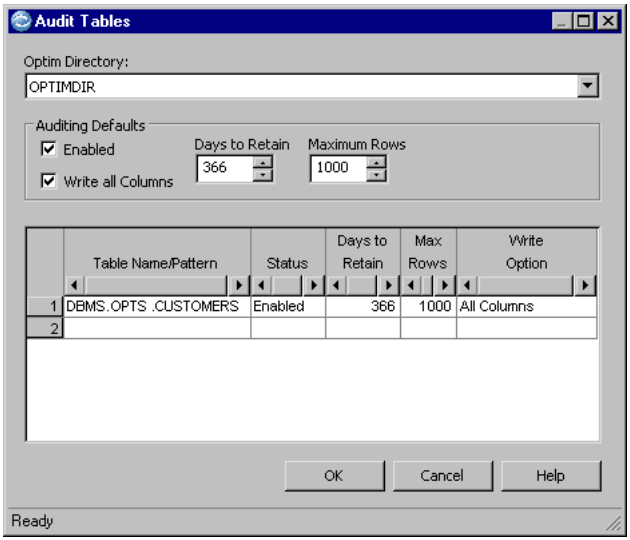
In **Browse** or **Edit** mode, a table can appear only once in the Table Editor. In **Browse Only** mode, a table can appear more than once in the Table Editor.

You can switch from **Browse Only** mode to **Browse** or **Edit** mode by unjoining any duplicate tables, selecting **Preferences** from the **Tools** menu on the Table Editor, and selecting **Browse** or **Edit** mode.

Note: If the **Force Browse Only** check box on the **Edit** tab in Product Options is selected, the controls pertaining to editing data are unavailable.

Audit Tables Dialog

If you select the **Auditing Active** check box on the **Edit** tab, click **Audit Tables** to display the **Audit Tables** dialog. You can specify a Personal Options list of tables to audit.



Note: Auditing is available in Personal Options only if the **Auditing Status** in Product Options is set to **Active/User**.

Optim Directory

Select the ***Optim*** Directory associated with the tables to audit. If you have access to more than one ***Optim*** Directory and want to specify the tables to audit for those directories, click the down arrow.

Audit results are stored in the PSTAUDIT table, which is one of the ***Optim*** Directory tables created when you install ***Optim***. If you are authorized, you can browse or edit the PSTAUDIT table in the same way you browse or edit any other database table. However, **Auditing Status** in Product Options must be set to **Active/User**, and you must have database SELECT authority for the PSTAUDIT table.

You can specify a Personal Options list of tables to audit. However, the list specified in Product Options takes precedence over the list that you specify in Personal Options.

Table Name/Pattern — Enter the name of the database table or pattern that identifies the tables to audit. Table names consist of *dbalias.creatorid.tablename*.

When you specify a pattern for like-named tables, you can use percent (%) to represent one or more characters. Use underscore (_) to represent a single character.

Note: An option on the **General** tab in Personal Options allows you to use the underscore as an SQL LIKE character.

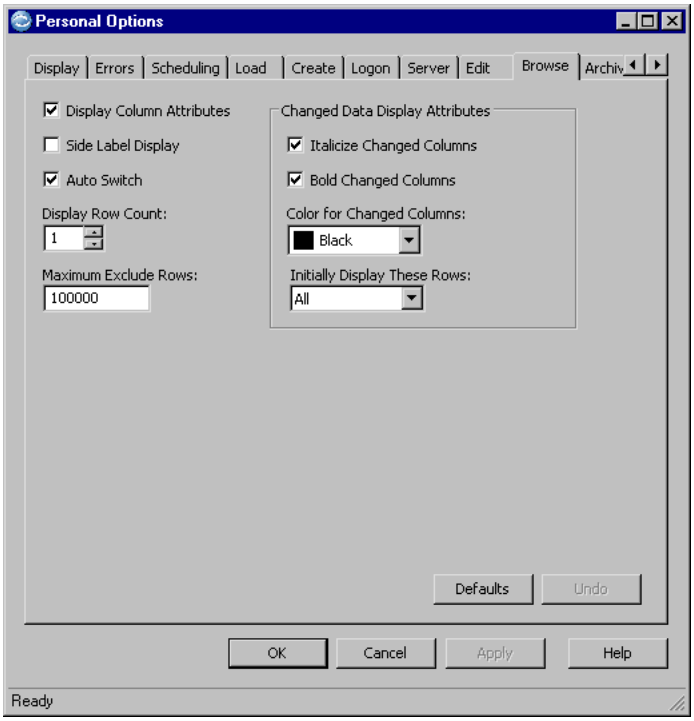
Status — Enable or disable the Audit option for individual tables. Click to display a down arrow and select **Enabled** or **Disabled** for each table in the list.

If the status indicates **Superseded by Product List**, the table is ignored because of a conflict with the parameters set in Product Options. You cannot enable or disable the audit option for that table, but you can modify the table name or remove it from the list.

The Edit Process audits tables based on a number of specific parameters, beginning with the parameters specified on the **Edit** tab in the **Product Options** dialog. Refer to **8.2.5 Edit Tab** on page 259 for more information about the Audit option.

9.2.11 Browse Tab

Use the options on the **Browse** tab to set preferences for browsing data and to select font characteristics for browsing a Compare File to quickly identify changed data.



Display Column Attributes

Select to display the data type, length, and nullable attributes for all columns in a selected table when browsing an Extract File, Archive File, or a Compare File. To display only column names, clear the check box.

Side Label Display

Select to display rows one at a time, with column names and values side-by-side. To display multiple rows, in a columnar format, clear this check box.

Auto Switch

Select to automatically switch subordinate tables in a stack of two or more joined tables to display related rows.

When you select a row in a table and there are no related rows in the subordinate table, the display is automatically switched to the next table in the stack that has a related row.

Display Row Count

Specify the default number of rows to display for each joined table. Use row count to manage the display area when you join several tables.

Maximum Exclude Rows

Specify a row limit to improve performance when browsing an Extract, Archive, or Control File that contains a large number of rows. When browsing, the **Exclude Rows** and **Only Show Rows in Error** features are unavailable for tables that exceed the specified row limit. (When an Extract, Archive, or Control File is first opened for browsing, system resources are allocated for creating a cache for temporary storage of excluded rows and rows in error. Therefore, browsing a very large file can consume a large amount of system resources.) This limit is reevaluated when a table is joined to another table, because the resulting subset may contain less rows.

The default value is 100,000 rows.

When a table is browsed that contains rows in excess of the **Maximum Exclude Rows** value, a message displays to remind you of the specified limit.

Note: If you never expect to use the **Exclude Rows** or **Only Show Rows in Error** features, set this limit very low to optimize system performance.

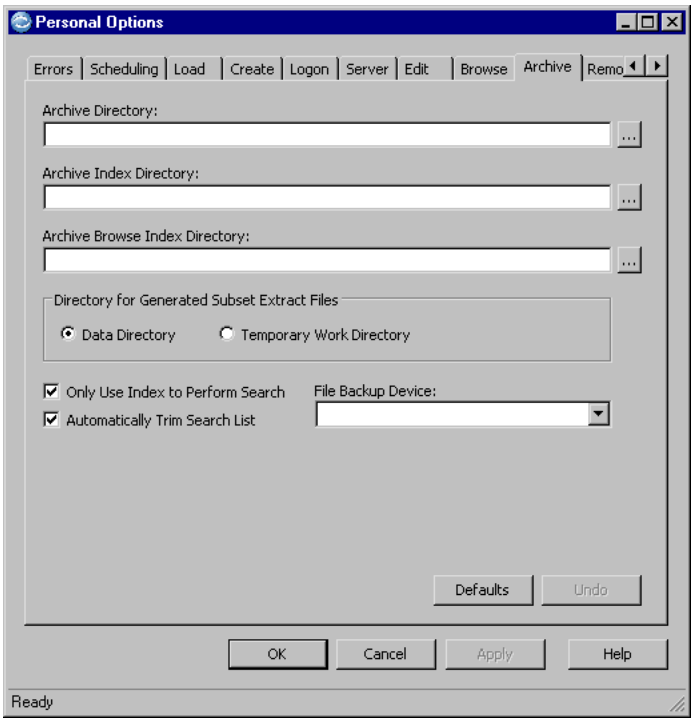
Changed Data Display Attributes

Select options to identify changed data when browsing a Compare File.

Italicize Changed Columns	Select to *italicize* data that differs between Source 1 and Source 2.
Bold Changed Columns	Select to display the data that differs between Source 1 and Source 2 in **bold** type.
Color for Changed Columns	Click the down arrow to select a color to identify data that differs between Source 1 and Source 2.
Initially Display These Rows	Select rows to display by default when browsing a Compare File: All, Different, Duplicate, Equal, or Only (unmatched rows).

9.2.12 Archive Tab

Use the options on the **Archive** tab to set preferences for an Archive Process.



Archive Directory

Specify the complete path to the default directory where you want to store Archive Files. To select from your system directories, click the browse button. If you do not specify a directory, the Data Directory specified on the **General** tab is used by default.

Archive Index Directory

Specify the complete path to the default directory where you want to store Archive Index Files. To select from your system directories, click the browse button. If you do not specify a directory, the Archive Directory is used by default.

Archive Browse Index Directory

Specify the complete path to the default directory where you want to store Archive Index Browse Files. To select from your system directories, click the browse button. If you do not specify a directory, the Archive Directory is used by default.

An Archive Index Browse File is created automatically whenever you join tables while browsing an Archive File. The Archive Index Browse

File stores primary key and foreign key information to expedite the retrieval of data, and has an *.abf* extension, by default. Archive Index Browse Files are dynamically updated. For this reason, it is advisable to select a directory accessible to any user that may browse an Archive File.

Directory for Generated Subset Extract Files

Select either **Data Directory** or **Temporary Work Directory** to specify the location in which to store automatically generated subset Extract Files.

Note: Both directories are specified on the **General** tab.

Only Use Index to Perform Search

When search criteria is used to locate Archive Files containing specific data, ***Optim*** initially searches for matching rows in the corresponding Archive Index Files. If a match for the search criteria cannot be determined from the Archive Index information (or index information is not defined), ***Optim*** must check the Archive File to resolve the search. This check box is cleared by default to direct the Archive Process to automatically search Archive Files when a match cannot be determined from Archive Index Files.

When you select this check box, you direct the Archive Process to search Archive Index Files only. Use shortcut menu commands **Resolve** and **Resolve All** to complete the search when a match cannot be determined from Archive Index information.

Automatically Trim Search List

Select to automatically exclude all files other than possible matches when you use the Search command to locate and display Archive File names that contain specific data.

File Backup Device

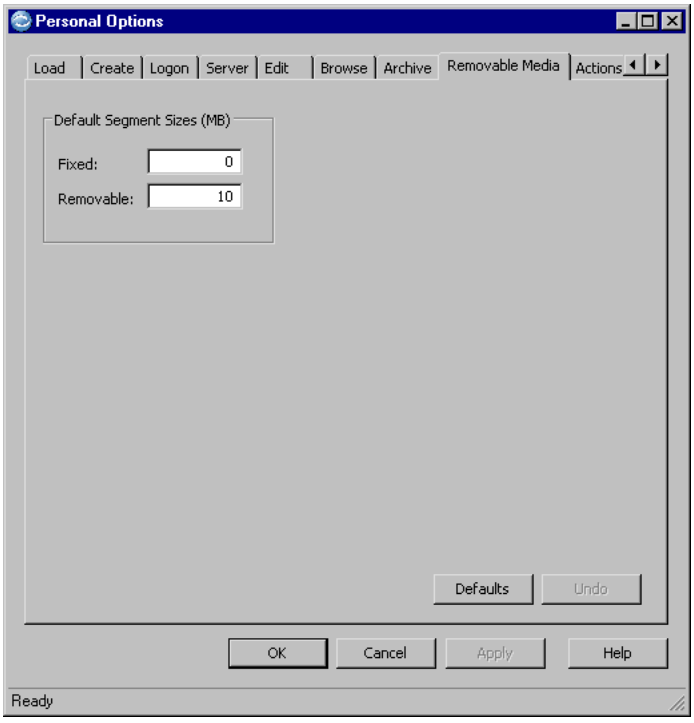
Click the down arrow to select the default backup device from a drop-down list of available backup devices.

Note: The drop-down list includes the backup devices selected on the **Archive** tab in Product Options. If no backup devices are selected in Product Options, this option is unavailable.

The default backup device is automatically selected when you create a new Storage Profile.

9.2.13 Removable Media Tab

Use options on the **Removable Media** tab to set default values for segment size when creating Archive Files, whether or not using a Storage Profile Definition, and Extract Files. When an Archive or Extract File is larger than the space limitation for the target media, the file must be segmented to span more than one volume.



Default Segment Sizes (MB)

Fixed Enter the segment size (0 - 9999 MB) to use when the target destination is a fixed drive (i.e. hard disk). To specify no limit, enter a value of 0 (zero).

Notes:

- This value also applies to Archive Files copied to a backup device, because Archive Files are created on disk before being copied to a backup device.
- The maximum segment size when the target is a Centera Server is 2 GB.

Removable Enter the segment size (1 - 9999 MB) to use when the target destination is a removable device (e.g., zip drive).

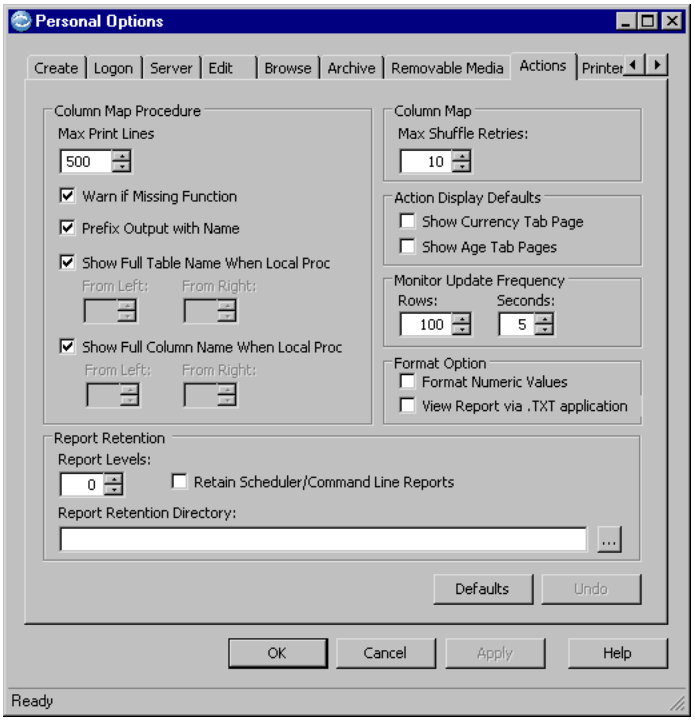
Note: The naming convention for a segmented file is: *filename*_1.*ext*, *filename*_2.*ext*, (... *filename_n.ext*), *filename.ext*. The name of the last segment is the file name specified in the process request. For example, when creating an Archive File named c:\arch\archtest.af that requires three segments, the segments are named as follows:

c:\arch\archtest_1.af (segment 1)
c:\arch\archtest_2.af (segment 2)
c:\arch\archtest.af (segment 3)

9.2.14 Actions Tab

Use the options on the **Actions** tab to select preferences for printing Column Map procedures, displaying tabs in Action Request Editors,

updating the Progress dialog, formatting numeric values, and retaining process reports.



Column Map Procedure

Max Print Lines Specify the maximum number of lines to route to a process report. If the number of lines exceeds this maximum, a warning message indicates the output is incomplete.

Warn if Missing Function Clear this check box to suppress the warning message generated in the process report when a Load, CmStartTable, CmEndTable, or UnLoad function is omitted from a Column Map Procedure.

Note: The CmTransform function must be included in a Column Map Procedure.

Prefix Output with Name Select the check box to include the name of the Column Map procedure with the print output (default).

Note: When you choose to include the name of the Column Map procedure with the print output, and a Local (i.e. unnamed) Column Map procedure is used, a name for the Local Column Map procedure is automatically generated. The name is generated using the corresponding table name, column name, and a unique number as follows: ***tablename.columnname.n***

The following options allow you to modify parts of the generated name for a Local Column Map procedure (the full table name and column name are used by default).

Show Full Table Name When Local Proc Select this check box to include the full table name in the generated Local Column Map procedure name.

If you clear this check box, use the **From Left** and **From Right** controls to specify a subset of the table name. **From Left** indicates the number of bytes to use from the beginning of the table name. **From Right** indicates the number of bytes to use from the end of the table name. (For example, if the table name is CUSTOMERS, and you specify 4 for **From Left** and 2 for **From Right**, the subset of the table name used is CUSTRS.)

Show Full Column Name When Local Proc Select this check box to include the full column name in the generated Local Column Map procedure name.

If you clear this check box, use the **From Left** and **From Right** controls to specify a subset of the column name. **From Left** indicates the number of bytes to use from the beginning of the column name. **From Right** indicates the number of bytes to use from the end of the column name. (For example, if the column name is SALESMAN_ID, and you specify 0 for **From Left** and 2 for **From Right**, the subset of the column name used is ID.)

Note: You can specify 0 for **From Left** and 0 for **From Right** to indicate that no part of the name is used. However, you must use part of either the table name or the column name.

Column Map

Max Shuffle Retries

Default number of times the Column Map Shuffle Function will refetch a replacement value until a value that does not match the source row is found (a "retry"). The Shuffle Function **retry** parameter overrides this default.

Enter a value from 0-1000. Enter 0 to allow a replacement value to match the source. The default is 10.

Note: Using a high retry value with columns that contain many duplicate values will increase the processing time. For these columns, it may be best to use a retry value of zero.

Action Display Defaults

Show Currency Tab Page — Select to display the **Currency** tab in the Convert, Insert, and Load Request Editors.

Show Age Tab Pages — Select to display the Age Function and Global Aging tabs in the Convert, Insert, and Load Request Editors.

Note: You can override these selections with commands available from the **Options** menu in each Action Request Editor.

Monitor Update Frequency

Rows — Specify the number of rows (100 to 5000) to process before updating the status message on the Progress dialog. The default value is 100.

Seconds — Specify the number of seconds (5 to 60) to pass before updating the process time on the Progress dialog. The default value is 5.

Format Numeric Values

Select this check box to format numeric values displayed on progress dialogs and in process reports for all actions. Clear this check box to display numeric values without formatting (e.g., 99888).

For example, if you select this check box and run the Extract Process, the **Extract Request Progress** dialog would display 99,888 for the total number of rows extracted, depending on the numeric format defined for Windows.

Note: To view the numeric format for your workstation, select **Regional Options** from the Control Panel and review the **Numbers** tab.

Report Retention

Report Levels — Specify the maximum number of reports you can retain for each type of process. You can specify a value from 0 through 200. A value of 0 (default) disables the report retention feature.

When the number of retained reports for a particular type of process exceeds the maximum, the oldest report is deleted and the current report is saved.

Retain Scheduler/ Command Line Reports	Select to retain reports generated by processes invoked using the the **Scheduler** or the Command Line Interface. This check box is cleared by default.
Report Retention Directory	Specify the complete path to the default directory in which you want to store reports. Leave blank (default) to use the Temporary Work Directory specified on the **General** tab. To select from your system directories, click the browse button. ***Note:*** It is recommended that each user specify a private directory for storing reports.

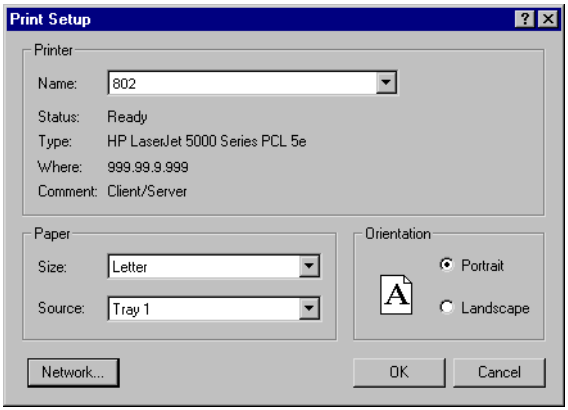
9.2.15 Printer Tab

Use the **Printer** tab to set printer, font, and language preferences for printing a request or definition. Note that font and language settings appropriate to the character set used for a request or definition will ensure that text prints correctly if the Locale settings for your computer do not match settings for the computer used to create the object.

The default printer and font information for requests and definitions are shown in each of the message boxes. To open the Windows **Print Setup** dialog to select a printer, click **Set Printer**. To open the Windows **Font** dialog to select font attributes and specify the desired language script, click **Set Font**.

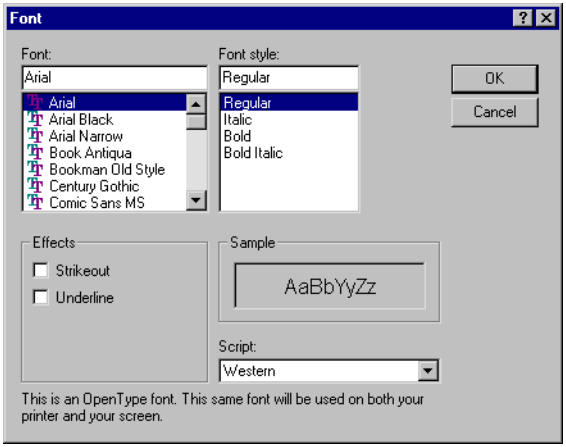
Printer

Set Printer Click to display the **Print Setup** dialog. Select a printer to use as the default when printing requests or definitions.



Field Font

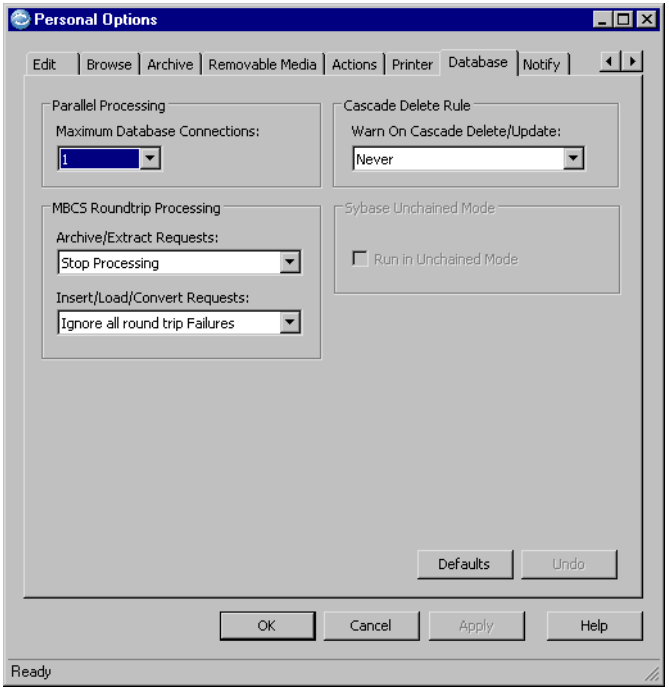
Set Font Click to display the **Font** dialog. Select font characteristics and a language script to use when printing requests or definitions.



Note: The available languages in the **Script** drop-down list are determined by the selected font.

9.2.16 Database Tab

Use the options on the **Database** tab to set preferences for handling database connections, multi-byte round trip conversion errors, and cascade deletes. For Sybase ASE, you can specify whether to run in Unchained mode.



Parallel Processing

Maximum Database Connections

Specify the default number of concurrent database connections for an Archive, Delete, or Extract Process. Increasing database connections improves performance when processing large quantities of data by allowing multiple threads to process rows in parallel.

To increase the maximum number of connections, select an even number from 2 through the site maximum as specified in Product Options.

Note: For performance reasons, you can only select an even number of maximum database connections.

MBCS Roundtrip Processing

Options for handling characters that could cause round trip conversion issues in a multi-byte ***Optim*** Directory or DB Alias. The availability of these options is governed by the **MBCS Roundtrip Processing** settings on the Product Options **Database** tab.

Optim uses the Unicode character set in dialogs and to process data. In some multi-byte character sets (such as Oracle JA16SJIS), multiple characters are mapped to the same Unicode character. When these characters are converted from Unicode back to multi-byte (a round trip), the original character may not be returned.

Archive/Extract Requests

Select an option for handling round trip conversion issues during Archive or Extract processing:

Stop Processing	Stop processing when a multi-byte character is encountered that could cause an incorrect round trip conversion.
Ignore all round trip Failures	Continue processing when a multi-byte character is encountered that could cause an incorrect round trip conversion. (Default.)

Insert/Load/ Convert Requests

Select an option for handling round trip conversion issues during Insert, Load, or Convert processing:

Stop Processing	Stop processing when a multi-byte character is encountered that could cause an incorrect round trip conversion.
Ignore all round trip Failures	Continue processing when a multi-byte character is encountered that could cause an incorrect round trip conversion. (Default.)

Select the **Ignore all round trip Failures** option if the database does not contain data with characters that could cause round trip errors, or if columns used to manipulate data in a Column Map (e.g., a function is used) and columns for which selection criteria are defined do not contain characters that could cause round trip errors.

Cascade Delete Rule

Warn On Cascade Delete/ Update

Display a warning if a cascading delete or update may occur to a table that is not explicitly included in an Access Definition or a process.

Runtime	Display a cascade delete/update warning only at run time of a process.
Saving Access Definition	Display a cascade delete/update warning only when saving the Access Definition.
Always	Display a cascade delete/update warning at run time of a process and when saving the Access Definition.
Never	Do not display a cascade delete/ update warning. This is the default setting.

The **Warn on Cascade Delete/Update** setting in Product Options (see **Cascade Delete Rule** on page 250) affects the availability of this option for user input. If available, you can click the down arrow to

choose when to display a warning. If unavailable, the value specified for **Warn on Cascade Delete/Update** in Product Options is displayed and cannot be modified.

Sybase Unchained Mode

Run in Unchained Mode

Optim normally runs in chained mode. When a trigger in a Sybase ASE table will be fired as a result of an Insert or Delete Process, and the trigger calls a stored procedure that must run in unchained mode, the connection must be in unchained mode for the procedure to work.

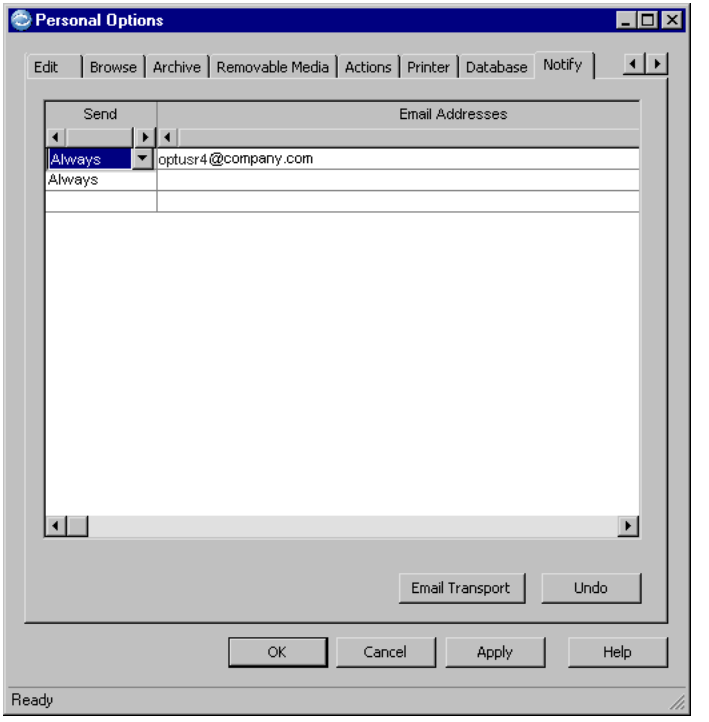
The **Sybase Unchained Mode** setting in Product Options (see **Sybase Unchained Mode** on page 252) enables or disables this check box. If enabled, select the check box to run Insert and Delete Processes in Unchained Mode, or clear the check box to run all actions in normal mode.

9.2.17 Notify Tab

Use the **Notify** tab to provide default options and addresses for automatic email notification of the success or failure of a process. The process report generated when a process completes is automatically sent as an attachment.

Note: Before using email notification, the desired email program must be installed. For Windows, the email client must be defined as the default, and set up to interface with MAPI. For UNIX or Linux, a valid copy of SENDMAIL must be configured correctly.

In an Action Request Editor, you can click **Get Site Defaults** on the **Notify** tab to populate it with the defaults specified in Personal Options.



Grid Details

The **Notify** tab contains the following details:

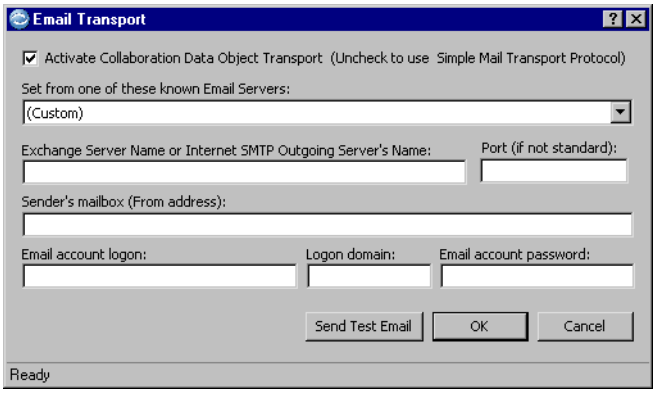
Send For each email address you list, click to select an option to send a message as determined by the outcome of the process. You can select **Always**, **Success**, or **Failure**.

Email Addresses Enter an email address to which notification is sent with a process report at the completion of the process. Enter one address per line.

Send Test eMail Right-click a grid row and select **Send Test eMail** to validate the email address.

Email Transport Click this button to display the **Email Transport** dialog so that you may activate and configure the Collaboration Data Object (CDO) transport to send email. If you don't click this button, email is sent using the Simple Mail Protocol Transport (SMTP).

Note: You must use the CDO transport if the email client on the server requires logon credentials to send an unattended message or requires user input when SMTP is used to send a message. Also, select the CDO option if the server uses a Microsoft Outlook client (version 2000 or later) to send messages through a Microsoft Exchange server.



Activate Collaboration Data Object Transport If you use the SMTP email transport, keep this check box cleared (default) and select **OK**. A popup will ask you if you want to connect without entering a password. If you use the CDO email transport, select this check box to enable the dialog and continue entering information.

Set from one of these known Email Servers Click to select an account from the list and populate the remainder of the **Email Transport** dialog with information for the selected account.

Exchange Server Name or Internet SMTP Outgoing Server's Name Type an exchange server name or internet address.

Port (if not standard)	Type a port name or leave blank (default port).
Sender's mailbox (From address)	Type the sender (From) email address.
Email account logon	Type the email logon name.
Logon domain	Type the domain name.
Email account password	Type the password. A blank password is valid if the account allows it; a prompt will confirm that you want to connect without entering a password.
Send Test Email	Click this button to send a test email to your mailbox.

Note: It is recommended that you send a test email to ensure that the information you entered is sufficient to send an email. If you do not receive the test email, make the necessary corrections to the information you entered.

Appendix A. Install and Configure the *Server* under UNIX or Linux

This appendix provides information needed to install and configure the ***Optim Server*** on a machine using the Sun Solaris operating environment under SPARC; the Hewlett-Packard HP-UX operating environment; the IBM AIX operating environment; or the Red Hat Application Server. Note that an ***Optim Server*** installed in a UNIX environment cannot access an ***Optim*** Directory in an SQL Server database.

Configuration files, included with the installation, must be modified to adapt the ***Server*** to the requirements of your environment.

After completing the installation and configuration, processing initiated on a Windows workstation can be directed to the ***Server***. Additionally, processing can be initiated via ODBC or from a console using a Command Line Interface.

Reinstalling in IBM AIX environment

When you install ***Optim*** 6.5 and sign a user exit, an entry is made in the AIX cache. If you need to reinstall ***Optim*** 6.5, you must remove this entry before reinstalling:

1. Log in as the root user.
2. From the console, enter this command:

   -s /*usr/sbin*/slibclean

   where */usr/sbin* is the ***Optim*** install directory.

Installing from a Network Drive

You can copy the contents of the ***Optim Server*** CD to a network drive and then run the **setup** program from the network drive. To copy to a network drive

1. Create a directory on a network drive.

2. Copy the contents of the ***Optim Server*** CD to the directory. Copy all of the files in the root of the ***Optim Server*** CD to the network drive.

3. See Section **A.1.1 Run Setup** to begin installation.

A.1 Installation

Installing the ***Server*** takes only a few minutes and can be performed using a graphical interface or from the command line.

- The graphical interface option uses the **setup** program to guide you through the installation process. To use this option, see **A.1.1 Run Setup**.

  Note: A graphical workstation is required to run the **setup** program, and a defined DISPLAY environment variable must point to the workstation. To ensure that you have the proper environment for running **setup**, open a terminal session and issue the following command: `echo $DISPLAY`. The command should return a valid identifier for your graphical workstation. If not, see your System Administrator.

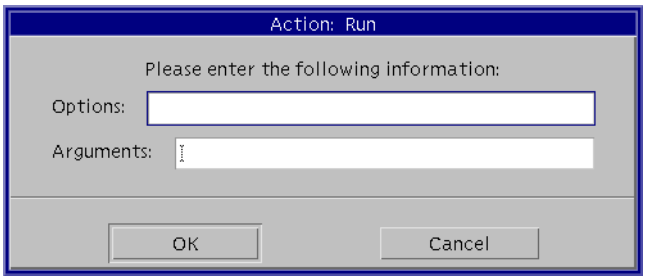
- The command line option uses a setup options file, *setupopts*, in which you define your installation settings. To use this option, see **A.1.2 Command Line Installation**.

A.1.1 Run Setup

You can begin ***Optim Server*** installation from a graphical interface in one of two ways:

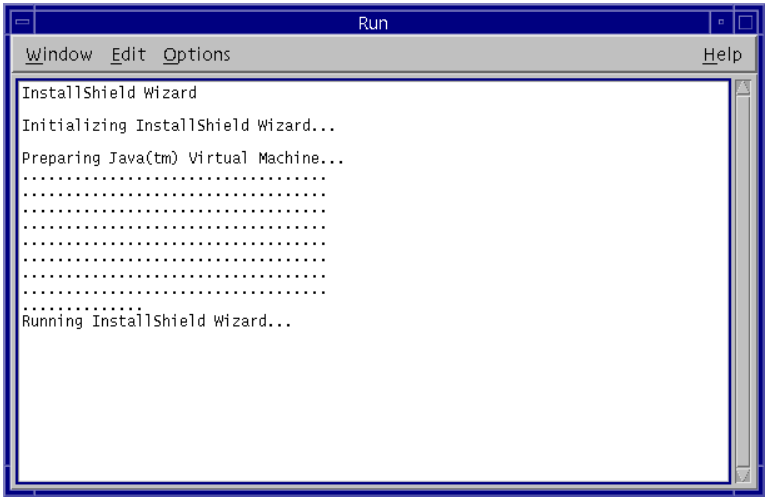
1. Mount the ***Optim Server*** CD. From File Manager or a console window, navigate to the CD-ROM drive and start **setup**.
2. If you copied the contents of the ***Optim Server*** CD to a network drive, navigate to the drive from File Manager or a console window, and start **setup**.

When you launch **setup**, a prompt for options and arguments displays.

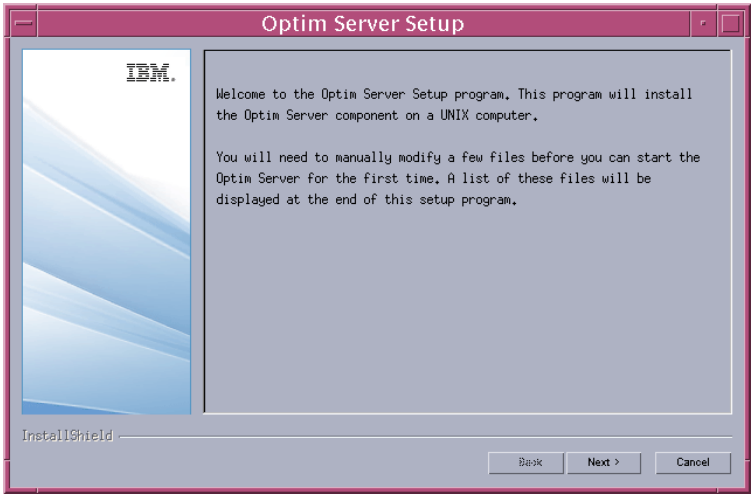


Do not enter options or arguments. Click **OK** to continue.

The progress of a Sun Java™ Runtime Environment, which launches an InstallShield Wizard, is displayed initially.



The InstallShield Wizard displays a Welcome panel. The Welcome panel reminds you that at the conclusion of the installation process, you must manually modify the configuration files before you can run ***Optim***.


Optim Server Setup
IBM
Welcome to the Optim Server Setup program. This program will install the Optim Server component on a UNIX computer.
You will need to manually modify a few files before you can start the Optim Server for the first time. A list of these files will be displayed at the end of this setup program.
InstallShield
Back
Next >
Cancel

Click **Next** to continue.

Troubleshooting Setup

If the InstallShield Wizard or Welcome panel fails to display, check the following:

- The DISPLAY environment variable must be set to a value that points to the graphical workstation session used to run the **setup** program.
- The signature of the mounted ***Optim*** CD must not contain the character "#". When Automount is used on a Sun Solaris machine to mount a CD, it creates a unique signature for the CD, which is usually the CD's volume label. If another CD with a matching volume label is mounted, Automount appends a *#n* to the end of the volume label to generate a unique signature. This can occur if two versions of an ***Optim*** CD are mounted, and UNIX has not been rebooted between mounts. If this occurs, you must shut down Automount and restart it.
- The temporary directory used by the **setup** program may be full. The default temporary directory is /var/tmp. To change the temporary directory, you can run the **setup** program with the following parameters:

  ./setup -is:tempdir /your_tmp_dir

  where "/your_tmp_dir" is the name of the temporary directory.

If the **setup** program still fails to start the InstallShield Wizard, you can run the **setup** program in console mode with the following parameters:

./setup -console -is:javaconsole

The default destination directory used by the **setup** program is

/opt/IBM/Optim

To change the destination directory in console mode, you can run the **setup** program with the following parameters:

./setup -console -is:javaconsole -P Main.installLocation=
/your_dest_dir

where "/your_dest_dir" is the name of the destination directory.

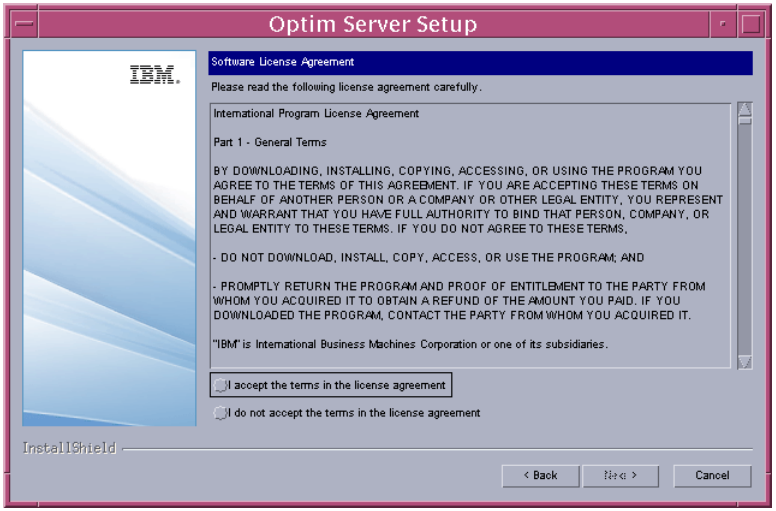
To change the temporary directory in console mode, you can run the **setup** program with the following parameters:

./setup -console -is:javaconsole -is:tempdir /your_tmp_dir

where "/your_tmp_dir" is the name of the temporary directory.

Software License Agreement

The next dialog prompts you to read the License Agreement.


Optim Server Setup
IBM.
Software License Agreement
Please read the following license agreement carefully.
International Program License Agreement
Part 1 - General Terms
BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, OR USING THE PROGRAM YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON OR A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON, COMPANY, OR LEGAL ENTITY TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,
- DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, OR USE THE PROGRAM; AND
- PROMPTLY RETURN THE PROGRAM AND PROOF OF ENTITLEMENT TO THE PARTY FROM WHOM YOU ACQUIRED IT TO OBTAIN A REFUND OF THE AMOUNT YOU PAID. IF YOU DOWNLOADED THE PROGRAM, CONTACT THE PARTY FROM WHOM YOU ACQUIRED IT.
"IBM" is International Business Machines Corporation or one of its subsidiaries.
I accept the terms in the license agreement
I do not accept the terms in the license agreement
InstallShield
< Back
Next >
Cancel

Command Buttons

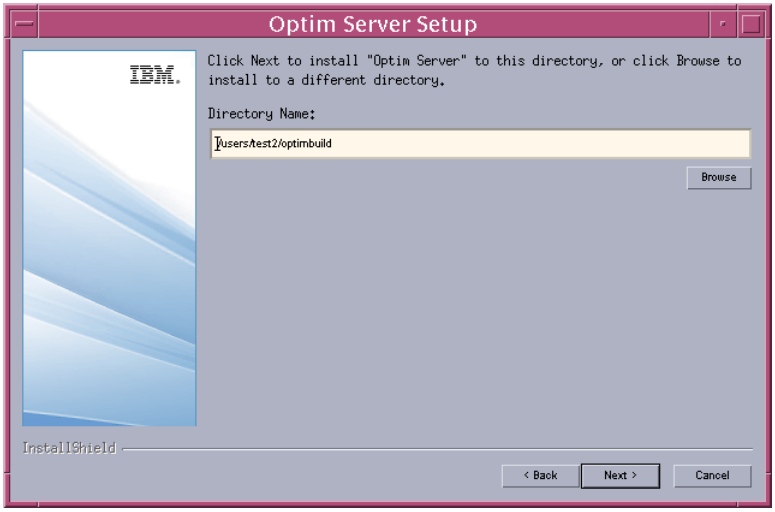
You must accept the terms of the license agreement in order to enable the **Next** button and continue the installation. After you select the option accepting the licensing agreement, click **Next** to indicate that your company agrees to its provisions. Other command buttons:

Back Close this dialog and return to the Welcome panel.

Cancel Cancel **setup**.

Choose Destination Location

The ***Server*** must be installed in a directory. When the following dialog opens, a default path and directory name are provided.



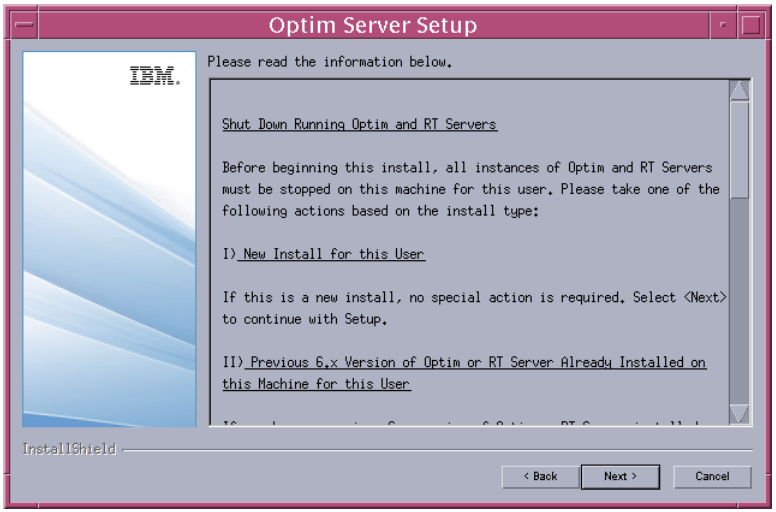
Directory Name Enter the directory path for installing the ***Server***. To change the path, type over the path provided, or click **Browse**. If you indicate a directory that does not exist, **setup** creates it. **Setup** also creates the subordinate directories, **RT** and **Bin**.

Browse Click **Browse** to open the **Choose Folder** dialog where you can select a different folder for installing the ***Server***.

To continue, click **Next**.

Shut Down the *Server*

If you are installing the ***Server*** for the first time or if you are re-installing a current version of the ***Server*** on a machine that has no other ***Server*** installations, simply click **Next** to continue with **setup**.


Optim Server Setup
IBM.
Please read the information below.
Shut Down Running Optim and RT Servers
Before beginning this install, all instances of Optim and RT Servers must be stopped on this machine for this user. Please take one of the following actions based on the install type:
I) New Install for this User
If this is a new install, no special action is required. Select <Next> to continue with Setup.
II) Previous 6.x Version of Optim or RT Server Already Installed on this Machine for this User
InstallShield
< Back
Next >
Cancel

However, if you are installing the ***Server*** in the same directory as any running ***Server*** or command line process, or you are running a ***Server*** or a command line process under the same user id that is running **setup**, you must stop one or more ***Optim Servers*** or ***Optim*** command line processes.

Before shutting a ***Server*** down, you must log on as the processing user account for the ***Server*** and run the following commands:

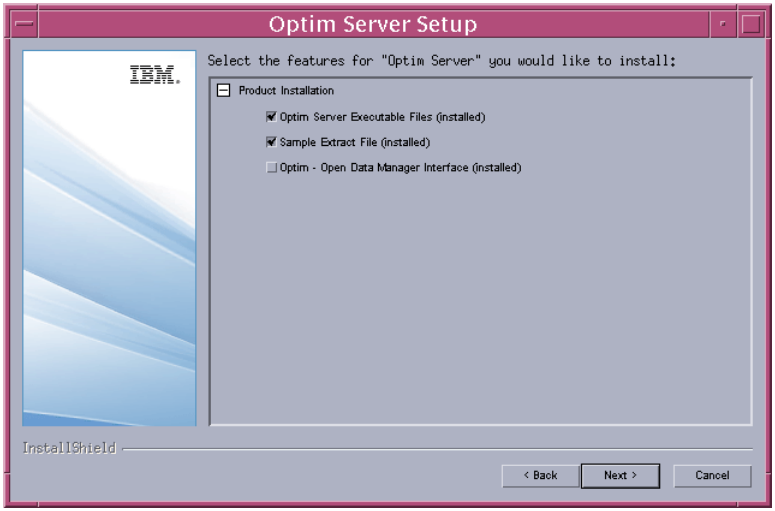
- **mwcleanup**
- **mwadm stop**.

If the services cannot be stopped because they are in use, you may see a message. You must then wait until the services end after all ***Optim*** command line processes that use them have exited and all ***Optim Servers*** that use them have been stopped. You can periodically check the status of the services with the **mwadm status** command.

If you want to force-stop the services, you can enter the **mwadm stop -f** command. However, use this command as the last resort as it will force terminate all running ***Optim*** programs that are using the services being stopped.

Select Components

The select components dialog lists the features available for installation. All components are selected by default.



Optim Server Executable Files

Select this check box to install all files, including shell scripts and configuration files, needed to run the ***Server*** in a Solaris, HP-UX, AIX or Linux operating environment.

Upon completion of the installation process, you are prompted to modify the shell scripts and configuration files to suit your environment.

Sample Files

Select this check box to install sample Extract Files. For more information about samples, refer to **Appendix H. Samples**.

Optim - Open Data Manager Interface

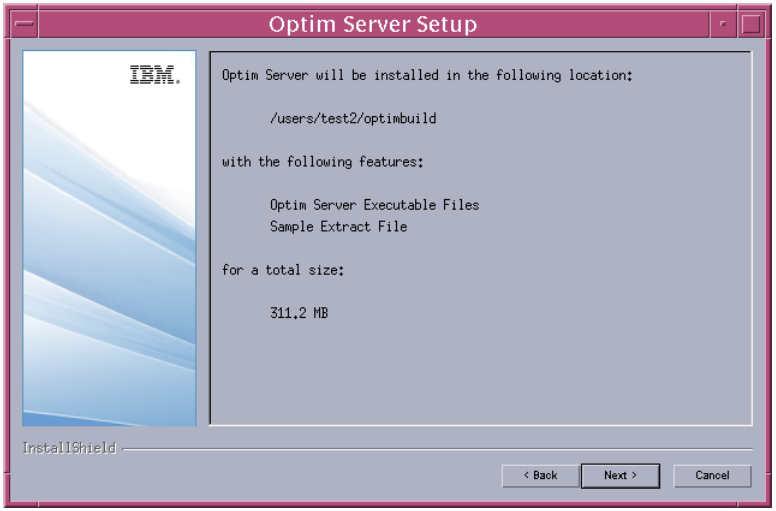
Select this check box to install Open Data Manager (ODM), which is used with external applications to access data in Archive Files. ODM requires a product license and is required for installations of certain ***Optim*** Application Aware Solutions. If ODM is needed, the Installation Guide for the ***Optim*** Application Aware Solution directs you to select ODM. Refer to **Appendix F. Open Data Manager** for ODM installation instructions.

To continue, click **Next**.

Confirmation

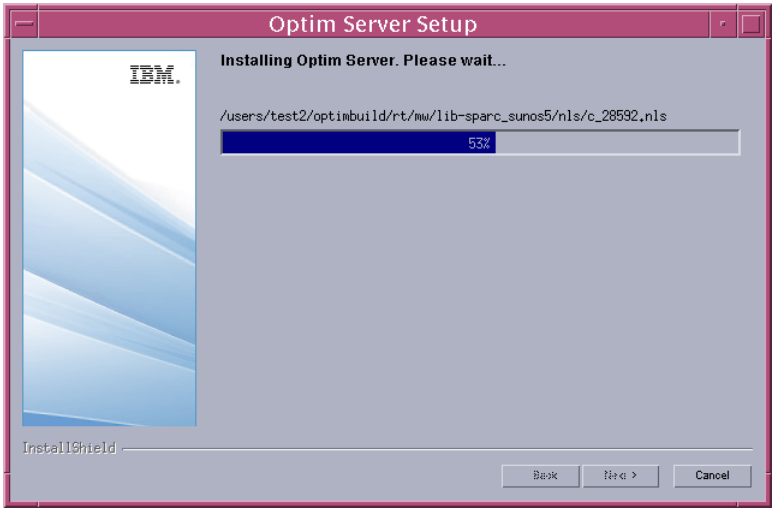
Setup displays the destination location, the features selected for installation, and the space required for your confirmation. To change

the destination or selection of features, click **Back** to return to the previous dialog.



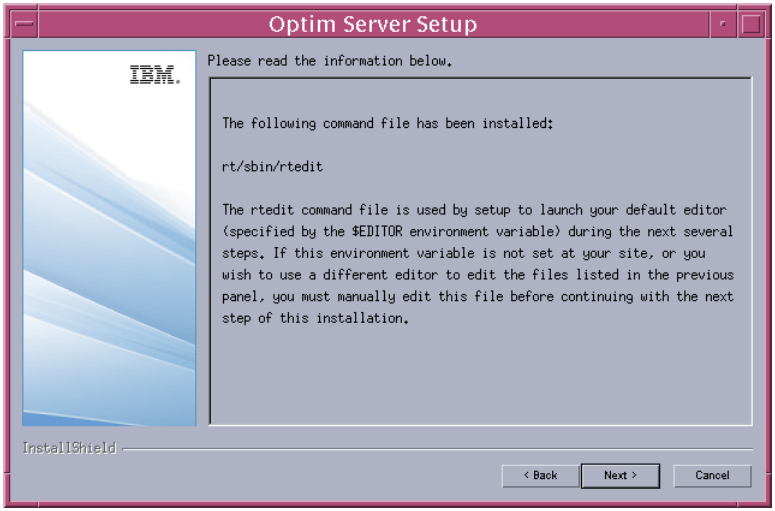
To begin the installation, click **Next**.

A progress indicator allows you to monitor the progress of the installation.

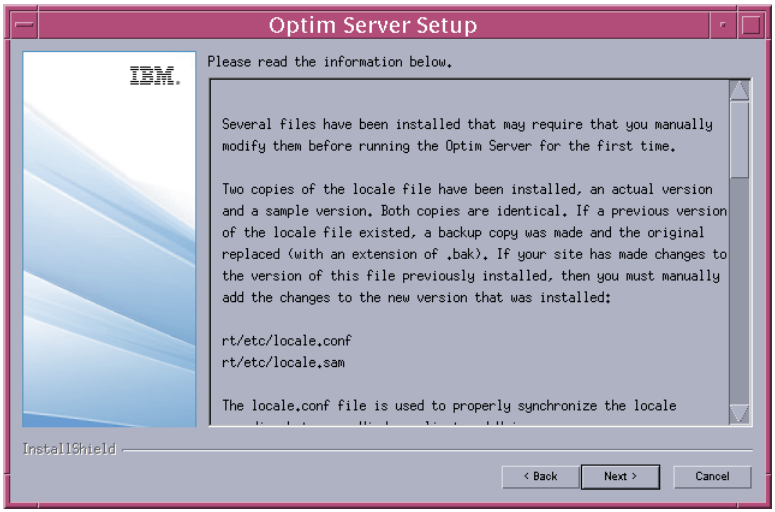


Edit Scripts and Configuration Files

You must modify shell scripts and configuration files before you can start the application the first time. **Setup** installs the rtedit command file to launch your default editor so that you can make these modifications.


Optim Server Setup
IBM.
Please read the information below.
The following command file has been installed:
rt/sbin/rtedit
The rtedit command file is used by setup to launch your default editor (specified by the $EDITOR environment variable) during the next several steps. If this environment variable is not set at your site, or you wish to use a different editor to edit the files listed in the previous panel, you must manually edit this file before continuing with the next step of this installation.
InstallShield
< Back
Next >
Cancel

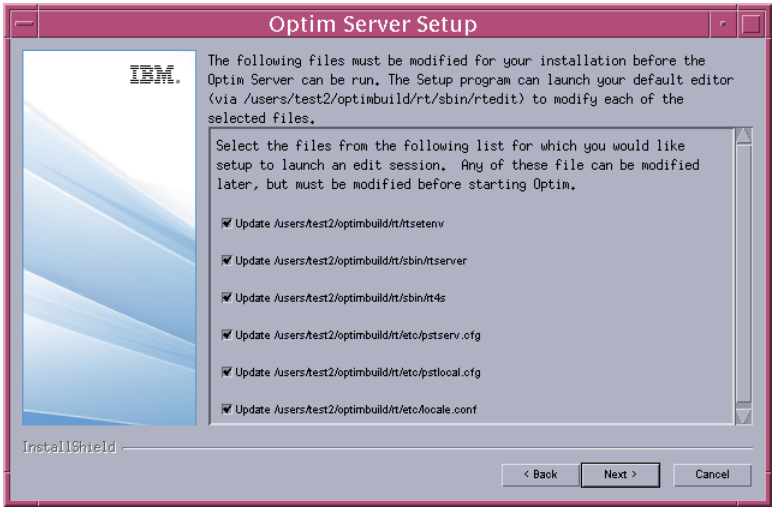
When you click **Next**, **setup** displays information about the shell scripts and configuration files to help you select files to modify. You can scroll the display to read information about each file.


Optim Server Setup
IBM.
Please read the information below.
Several files have been installed that may require that you manually modify them before running the Optim Server for the first time.
Two copies of the locale file have been installed, an actual version and a sample version. Both copies are identical. If a previous version of the locale file existed, a backup copy was made and the original replaced (with an extension of .bak). If your site has made changes to the version of this file previously installed, then you must manually add the changes to the new version that was installed:
rt/etc/locale.conf
rt/etc/locale.sam
The locale.conf file is used to properly synchronize the locale
InstallShield
< Back
Next >
Cancel

For new installations, a working version and a sample version of each shell script and configuration file are installed. The sample version of each file has the file extension *.sam*.

For upgrade installations, only the sample scripts and files are installed, and existing samples are automatically renamed with the extension *.bak*. This feature prevents overwriting of your working scripts and files, and allows you to compare existing versions with new sample versions.

When you click **Next**, you are prompted to edit each shell script and configuration file.


Optim Server Setup
IBM.
The following files must be modified for your installation before the Optim Server can be run. The Setup program can launch your default editor (via /users/test2/optimbuild/rt/sbin/rtedit) to modify each of the selected files.
Select the files from the following list for which you would like setup to launch an edit session. Any of these file can be modified later, but must be modified before starting Optim.
Update /users/test2/optimbuild/rt/rtsetenv
Update /users/test2/optimbuild/rt/sbin/rtserver
Update /users/test2/optimbuild/rt/sbin/rt4s
Update /users/test2/optimbuild/rt/etc/pstserv.cfg
Update /users/test2/optimbuild/rt/etc/pstlocal.cfg
Update /users/test2/optimbuild/rt/etc/locale.conf
InstallShield
< Back
Next >
Cancel

- The RTSETENV shell script is included in a user ".profile" or ".login" script to define the operating environment for the ***Server***. This script sets up the ***Server*** daemon or command line environment on login. A UNIX environment requires certain environment variables to create default settings. For detailed information needed to edit this file, refer to **A.2.3 RTSETENV Shell Script**.

- The RTSERVER shell script contains a series of useful commands that allow you to manipulate the ***Server*** process. This script does not need modification. For detailed information needed to edit this file, refer to **A.2.4 RTSERVER Shell Script**.

- The RT4S shell script is used to start or stop the ***Server*** from init(1) processing. This script should be executed only as part of the system boot procedure. Generally, the script does not need modification, unless the ***Server*** is installed in a directory other than the default

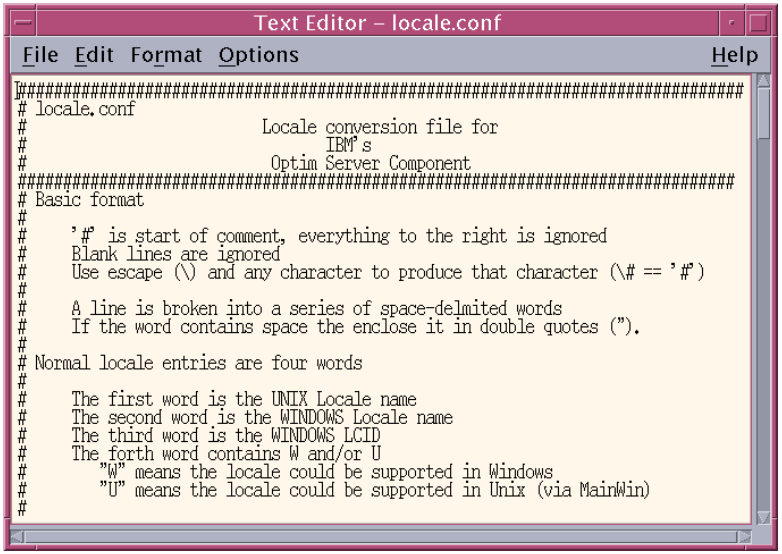
directory, `/opt/IBM/Optim`, or the ***Server*** will be run under a user account other than root. For detailed information needed to edit this file, refer to **A.2.5 RT4S Shell Script**.

- The pstserv configuration file (**pstserv.cfg**) is used to configure the system to run the ***Server*** daemon. Before you run the ***Server*** daemon, you must modify the file to reflect your site requirements. For detailed information needed to edit this file, refer to **A.2.1 Pstserv Configuration File**.

- The pstlocal configuration file (**pstlocal.cfg**) is used to configure the system for running the Command Line Utility or using the ODBC interface. For detailed information needed to edit this file, refer to **A.2.2 Pstlocal Configuration File for the Command Line Utility**.

- The locale.conf file provides locale conversion information between platforms. You can use this file to provide additional locale conversion information. For detailed information needed to edit this file, refer to **A.2.6 LOCALE.CONF Conversion File**.

If you choose to update a file, the default text editor is launched, displaying the corresponding file.

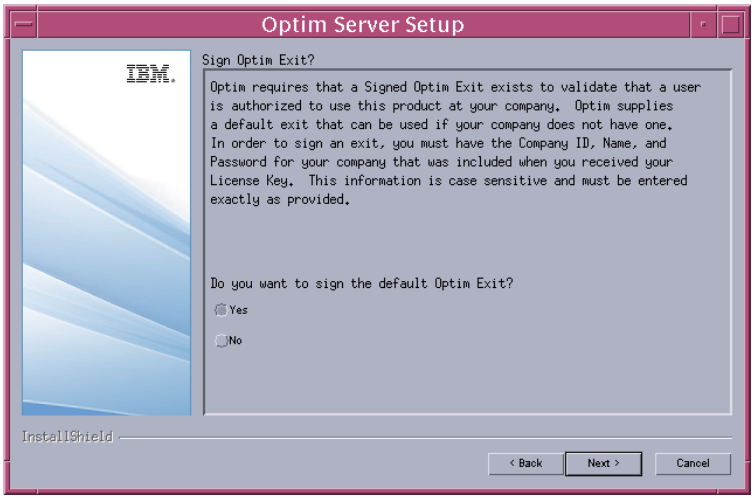

Text Editor – locale.conf
File Edit Format Options Help
locale.conf
Locale conversion file for
IBM's
Optim Server Component
Basic format
'#' is start of comment, everything to the right is ignored
Blank lines are ignored
Use escape (\) and any character to produce that character (\# == '#')
A line is broken into a series of space-delmited words
If the word contains space the enclose it in double quotes (").
Normal locale entries are four words
The first word is the UNIX Locale name
The second word is the WINDOWS Locale name
The third word is the WINDOWS LCID
The forth word contains W and/or U
"W" means the locale could be supported in Windows
"U" means the locale could be supported in Unix (via MainWin)

Note: InstallShield saves setup information in a file named **vpd.properties**, located in your home directory. This file contains information about the current ***Optim*** installation like

the options that have been installed and the ***Optim*** install directory. If you manually delete the ***Optim*** directory, you should also delete this file.

Sign the Optim Exit

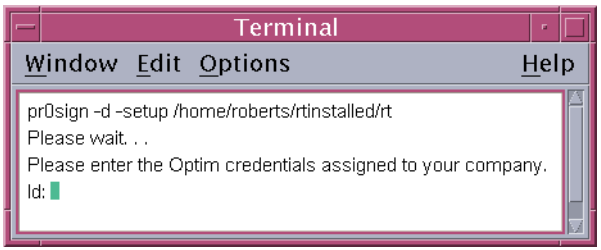
When the **Sign Optim Exit** dialog appears, click **Yes** to sign the default exit included with ***Optim*** or click **No** to skip this step; then click **Next**.


Optim Server Setup
IBM.
Sign Optim Exit?
Optim requires that a Signed Optim Exit exists to validate that a user is authorized to use this product at your company. Optim supplies a default exit that can be used if your company does not have one. In order to sign an exit, you must have the Company ID, Name, and Password for your company that was included when you received your License Key. This information is case sensitive and must be entered exactly as provided.
Do you want to sign the default Optim Exit?
Yes
No
InstallShield
< Back
Next >
Cancel

You must sign the default exit or a custom exit supplied by you to use ***Optim***, but you can only sign the default exit during setup. (See **A.5 The Optim Exit in UNIX** for detailed information on the ***Optim*** default exit and user-supplied exits.)

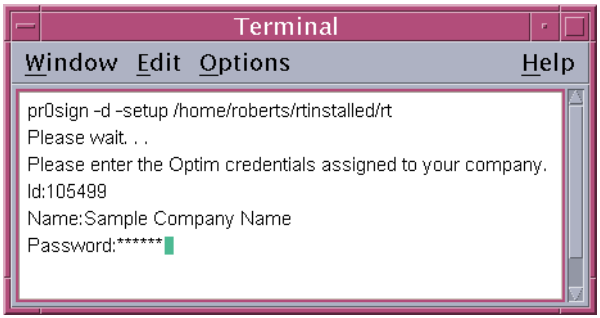
Note: If you want to sign a custom, user-supplied exit, you must run a script file called **opmusign** following installation, as described in **A.5.7 Signing a User-Supplied Exit in UNIX**.

If you select **Yes on** the **Sign Optim Exit** dialog to sign the default exit, setup will open a separate terminal window to sign the default exit.



Specify your Company ID, Name and Password

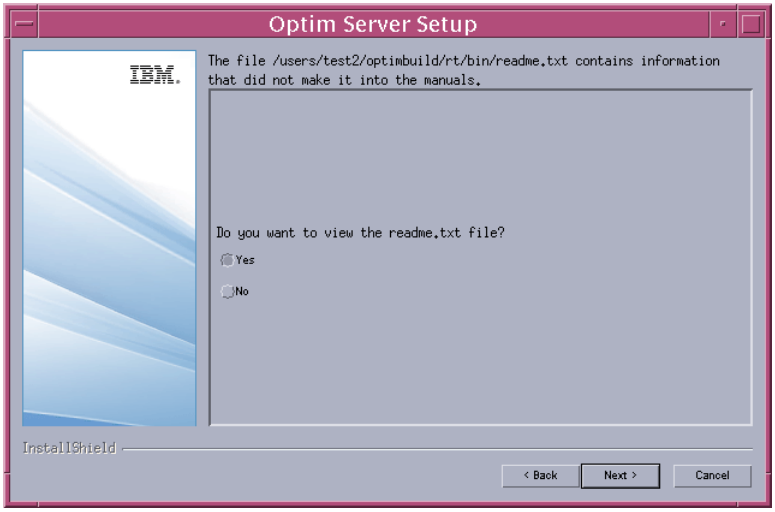
Type your company credentials when prompted for that information. Your company credentials consist of the company **Id**, **Name**, and **Password** assigned to your organization when you received ***Optim***. All three entries are case sensitive, and you must enter them in the format provided to you. Press **Enter** after each prompt to display the next prompt. After you specify your company **Id**, for example, press **Enter** to display the **Name** prompt.



Note: If any of the company credentials you specified are incorrect, an **Invalid Credentials Specified** dialog will prompt you to re-enter your credentials, as described in **A.5.4 The Invalid Credentials Specified Dialog** on page 407. If there are any other exit-related problems, a **Sign Optim Exit Failed** dialog will prompt you to correct those errors, as described in **A.5.5 The Sign Optim Exit Failed Dialog** on page 408.

Read Me

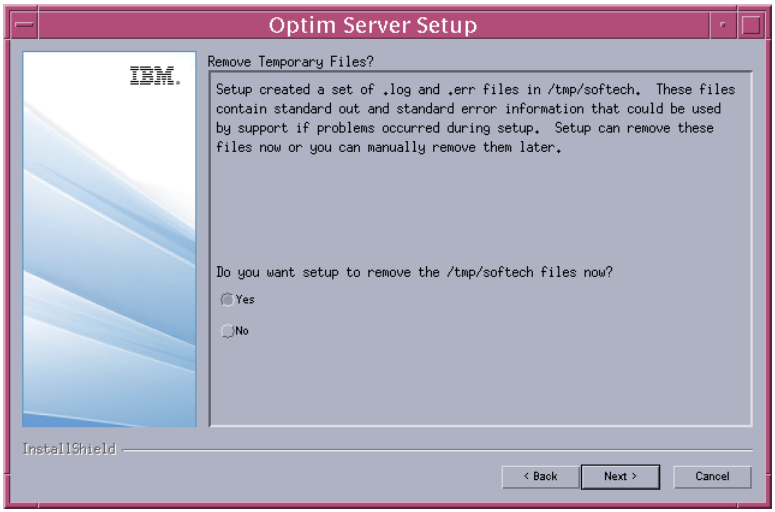
After editing and saving the files, you are prompted to view the readme.txt file, containing installation notes and information.



Remove Temporary Files

During installation, ***Optim*** creates several temporary log and error files, and stores those files in a **/tmp/softech** directory. ***Optim*** support personnel use those files to diagnose any problems encountered during installation. If installation was successful, you should remove those files when prompted to do so on the **Remove Temporary Files** dialog. (If you do not delete the temporary files and you do another install using a different user id, the old files will prevent the new files from being created.)

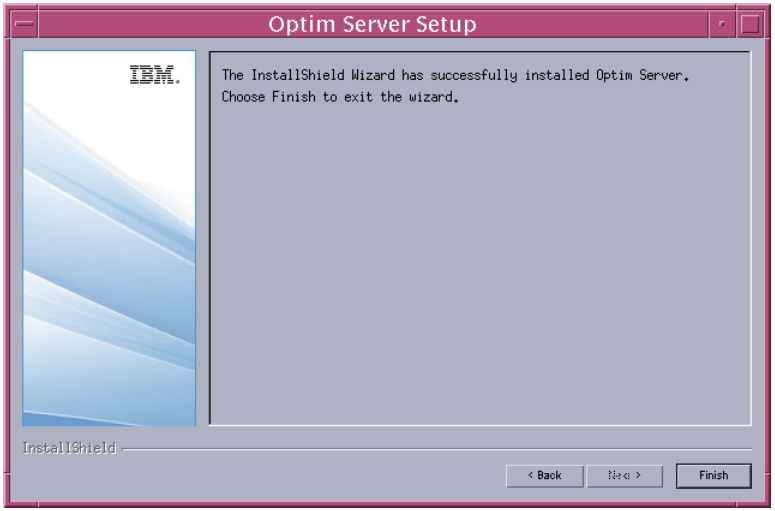
Select **Yes** and click **Next** on the **Remove Temporary Files** dialog to delete the temporary .log and .err files stored in the **/tmp/softech** directory, as indicated below.


Optim Server Setup
IBM.
Remove Temporary Files?
Setup created a set of .log and .err files in /tmp/softech. These files contain standard out and standard error information that could be used by support if problems occurred during setup. Setup can remove these files now or you can manually remove them later.
Do you want setup to remove the /tmp/softech files now?
Yes
No
InstallShield
< Back
Next >
Cancel

Note: The **/tmp/softech** directory only contains files concerning the installation of ***Optim***. It does not contain any files concerning the signing of the default exit; that information is stored in the **rt/temp** directory, so if installation was successful, you should delete the temporary files in the **/tmp/softech** directory, even if you did not sign the default exit.

Setup Complete

At the conclusion of the installation, a dialog indicates the ***Server*** has been successfully installed. Click **Finish** and close the console window to complete the installation process.



Click **Finish** and close the console window to complete the installation process.

A.1.2 Command Line Installation

To install the ***Server*** from the command line, use the setup options file, *setupopts*, located on the product CD.

Editing *setupopts*

To install the ***Server***, mount the product CD and copy *setupopts* from the root directory to a location for which you have write access. You can edit the file using an ASCII editor. Enable a keyword by removing the leading '###' characters from the line. Define a parameter for a keyword by editing the characters after the '='.

Installation

Run the setup process from the command line, using the following command:

```
./setup -silent -options <file-name>
```

For example, if *setupopts* is in the /users/name directory, enter the following:

```
./setup -silent -options /users/name/setupopts
```

If you are upgrading or installing on a machine that has one or more ***Servers*** installed in another directory, you must manually shut down all ***Server*** processing. To shut down a ***Server***, you must log on as the processing user account for each ***Server*** and run the following command before manually shutting the ***Server*** down.

```
rt/mw/bin/mwadm stop
```

Syntax

The syntax conventions used to describe *setupopts* are:

parameter	Parameters can be entered in UPPER, lower or Mixed case. Defaults are shown in **bold** text.
text	Variable parameter text is shown in lowercase italics.
[ ]	Delimiter for optional keywords or parameters.
{ }	Delimiter for a choice from which you must select one.
|	Separates options.

–W LicensePanel.selection={ **1** | 2 }
–P installLocation=*installdirectory*
[–P ProgramFeature.active=[**true** | false]]
[–P ODBCFeature.active=[**true** | false]]
[–P SampleFeature.active=[**true** | false]]
[–P ODMFeature.active=[true | **false**]]

[–W ConfigureODMPromptPanel.ConfigureODMChoice=[1 | **2**]]
[–W ODMLicensePanel.ODMLicenseField=*licensepath*]
[–W UpdateFilesPanel.Update_rtsetenv=[**0** | 1]]
[–W UpdateFilesPanel.Update_rtserver= [**0** | 1]]
[–W UpdateFilesPanel.Update_rt4s=[**0** | 1]]
[–W UpdateFilesPanel.Update_pstserv=[**0** | 1]]
[–W UpdateFilesPanel.Update_pstlocal=[**0** | 1]]
[–W UpdateFilesPanel.Update_locale=[**0** | 1]]
[–W View_Readme.Value=[**0** | 1]]

Keywords

–W LicensePanel.selection=

The ***Optim*** license agreement. You must accept the license agreement to continue the installation.

1 "I accept the terms of the license agreement."

2 "I do not accept the terms of the license agreement."

```
-W LicensePanel.selection=1
```

–P installLocation=

The directory path for installing the ***Server***. If the directory name contains spaces, enclose it in double-quotes.

```
-P installLocation=/opt/IBM/Optim/rt
```

–P ProgramFeature.active=

Install the ***Server***. This option installs all files needed to run the ***Server*** in a Solaris, HP-UX, or AIX operating environment, including shell scripts and configuration files.

true Install the ***Server***.

false Do not install the ***Server***.

```
-P ProgramFeature.active=true
```

–P ODBCFeature.active=

Install the ***Optim Archive*** ODBC Interface feature. Selecting this component registers the ***Optim Archive*** ODBC Interface driver with ODBC on your workstation.

Note: If an earlier version of ODBC is installed, selecting this component will upgrade the API.

true Install the ***Optim Archive*** ODBC Interface feature.

false Do not install the ***Optim Archive*** ODBC Interface feature.

```
-P ODBCFeature.active=true
```

–P SampleFeature.active=

Install sample Extract Files.

true Install sample Extract Files.

false Do not install the sample Extract Files.

```
-P SampleFeature.active=true
```

–P ODMFeature.active=

Install the ***Optim*** Open Data Manager (ODM) interface feature, which is used only with integrated applications such as ***Optim*** **Oracle E-Business Suite Solution**. ODM requires a product license. If you select this option, refer to **Appendix F. Open Data Manager** for ODM configuration instructions.

true Install the ***Optim*** ODM interface feature.

false Do not install the ***Optim*** ODM interface feature.

```
-P ODMFeature.active=false
```

Note: If you set **-P ODMFeature.active=true**, you must define a value for **-W ConfigureODMPromptPanel.ConfigureODMChoice**.

–W ConfigureODMPromptPanel.ConfigureODMChoice=

If the ***Optim*** ODM feature is installed, indicate when it is configured.

1 Configure ODM now. This option prompts you for the Attunity license file and automatically installs the ODM Server.

2 Configure ODM later. This option copies the ODM Server installation files to your machine. To complete the ODM Server installation, you must install the ODM Server and register the Attunity license manually.

```
   -W
ConfigureODMPromptPanel.ConfigureODMChoice
=2
```

Note: If you choose to configure ODM now, **-W ConfigureODMPromptPanel.ConfigureODMChoice=1**, you must define a value for **-W ODMLicensePanel.ODMLicenseField**.

–W ODMLicensePanel.ODMLicenseField=

If you choose to configure ODM now, **-W ConfigureODMPromptPanel.ConfigureODMChoice=1**, enter the fully qualified name to the Attunity Licence File. If the directory contains spaces, enclose it in double-quotes.

Note: If you do not have an Attunity license file, enter **-W ConfigureODMPromptPanel.ConfigureODMChoice=2**.

```
 -W ODMLicensePanel.ODMLicenseField=/opt/
ODM/license.txt
```

–W UpdateFilesPanel.Update_rtsetenv=

Edit the RTSETENV shell script during the installation process, using the default text editor.

The RTSETENV shell script is included in a user ".profile" or ".login" script to define the operating environment for the ***Server***. This script sets up the ***Server*** daemon or command line environment on login. The operating environment requires certain environment variables to create default settings. For detailed information needed to edit this file, refer to **A.2.3 RTSETENV Shell Script**.

0 Do not edit RTSETENV during installation.

1 Edit RTSETENV during installation. (If you are not installing from a graphical interface, this option will cause an error.)

```
-W UpdateFilesPanel.Update_rtsetenv=0
```

–W UpdateFilesPanel.Update_rtserver=

Edit the RTSERVER shell script during the installation process, using the default text editor.

The RTSERVER shell script contains a series of useful commands that allow you to manipulate the ***Server*** process. This script does not need modification. For detailed information needed to edit this file, refer to **A.2.4 RTSERVER Shell Script**.

0 Do not edit RTSERVER during installation.

1 Edit RTSERVER during installation. (If you are not installing from a graphical interface, this option will cause an error.)

```
-W UpdateFilesPanel.Update_rtserver=0
```

–W UpdateFilesPanel.Update_rt4s=

Edit the RT4S shell script during the installation process, using the default text editor.

The RT4S shell script is used to start or stop init(1) processing for the ***Server***. This script should be executed only as part of the system boot procedure. Generally, the script does not need modification, unless the ***Server*** is installed in a directory other than the default directory, `/opt/IBM/Optim`, or the ***Server*** will be run under a user account other than root. For detailed information needed to edit this file, refer to **A.2.5 RT4S Shell Script**.

0 Do not edit RT4S during installation.

1 Edit RT4S during installation. (If you are not installing from a graphical interface, this option will cause an error.)

```
-W UpdateFilesPanel.Update_rt4s=0
```

–W UpdateFilesPanel.Update_pstserv=

Edit the pstserv configuration file during the installation process, using the default text editor.

The pstserv configuration file (**pstserv.cfg**) is used to configure the system to run the ***Server*** daemon. Before you run that daemon, you must modify the file to reflect your site requirements. For detailed information needed to edit this file, see **A.2.1 Pstserv Configuration File**.

0 Do not edit pstserv during installation.

1 Edit pstserv during installation. (If you are not installing from a graphical interface, this option will cause an error.)

```
-W UpdateFilesPanel.Update_pstserv=0
```

–W UpdateFilesPanel.Update_pstlocal=

Edit the pstlocal configuration file during the installation process, using the default text editor.

The pstlocal configuration file (**pstlocal.cfg**) is used to configure the system for running the Command Line Utility or using the ODBC interface. For detailed information needed to edit this file, see **A.2.2 Pstlocal Configuration File for the Command Line Utility**.

0 Do not edit pstlocal during installation.

1 Edit pstlocal during installation. (If you are not installing from a graphical interface, this option will cause an error.)

```
-W UpdateFilesPanel.Update_pstlocal=0
```

–W UpdateFilesPanel.Update_locale=

Edit the locale.conf file during the installation process, using the default text editor. The locale.conf file provides locale conversion information between platforms. You can use this file to provide additional locale conversion information. For detailed information needed to edit this file, see **A.2.6 LOCALE.CONF Conversion File**.

0 Do not edit locale.conf during installation.

1 Edit locale.conf during installation. (This option will cause an error unless installing from a graphical interface.)

```
-W UpdateFilesPanel.Update_locale=0
```

–W View_Readme.Value=

Open the readme.txt file, using the default text editor. The readme.txt file contains installation notes and information.

0 Do not open readme.txt during installation.

1 Open readme.txt during installation. (If you are not installing from a graphical interface, this option will cause an error.)

```
-W View_Readme.Value=0
```

A.2 Configuration

Configuration files and shell scripts are installed with the **Executable Files** when you install the ***Server*** in a supported UNIX environment. These objects establish defaults for the ***Server*** and must be customized to reflect your network environment. Use a text editor (e.g., vi, emacs, CDE Text Editor, textedit, or xedit) to modify these files.

Configuration Files

Configuration files are ASCII text files and are installed in the `/etc` directory that is subordinate to the PSTHOME directory. PSTHOME is an environment variable, set during installation, that points to the directory in which the ***Server*** is installed.

The configuration file names for the ***Server*** are:

pstserv.cfg Configures prosvce, the ***Server*** daemon.

pstlocal.cfg Configures local command line and ODBC functionality.

The appropriate Configuration file is loaded and validated when prosvce, ODBC, or the Command Line Utility starts up. You can also use `pr0svce -v` to validate pstserv.cfg or `pr0cmnd -v` to validate pstlocal.cfg.

To reload the configuration file for prosvce while it is running, use `pr0svce -u` from a console under the user account for the daemon (or use `pr0svce -u` *`userid`* from root). After all clients have logged off, the file is read, reloaded, and validated. A console message and system log verify the file has been loaded.

Note: Use `pr0svce -L` (or use `pr0svce -L` *`userid`* from the root account) to determine if the system is waiting to reload.

Shell Scripts

The installed shell scripts are:

RTSETENV Defines the operating environment for the ***Server***. Installed in the PSTHOME directory and designed to be included in a user .profile or .login script to set up the environment for the ***Server*** or command line on login.

RTSERVER Provides commands that allow you to manipulate the ***Server*** process. Installed in `/sbin`, subordinate to the PSTHOME directory.

RT4S Used to start or stop the ***Server*** from init processing. Installed in `/sbin`, subordinate to the PSTHOME directory, RT4S should be executed only as part of the system boot procedure.

Conventions

The following conventions are used in shell scripts and .cfg files:

- One parameter per line.
- Blank lines and leading and trailing blanks within a line are ignored.
- Use double quotes or the escape character (\) to pass a special character to processing:
  - Enclose a string that includes '# ' in double quotes (e.g., "text#here").
  - To include a double quote (") within a quoted string, use the escape character, \, (e.g., \").
  - Precede a special character that is not in a quoted string with the 'escape' character, \, (e.g., \#, \\).
- References to environment variables are in the form ${*environmentvariablename*}. An environment variable that does not exist equates to a NULL string (" "). For example, AAA${NOT_EXIST}BBB is treated as AAABBB.
- Parameters and keywords are not case sensitive. Directories, file names, User IDs, and passwords are case sensitive.
- Keywords shown as 0 (zero) in the following text can also be entered as f, or false, while keywords shown as 1 can be entered as t, or true.
- Comments are allowed after an entry and must begin with '# '.

Syntax

The syntax conventions used to describe the configuration files, shell scripts, and commands are:

parameter Parameters and keywords can be entered in UPPER, lower or Mixed case.

text Variable text is shown in lowercase italics.

( ) Delimiter to group a series of qualifiers.

[ ] Delimiter for optional parameters or settings.

{ } Delimiter for a choice from which you must select one.

< > Delimiter for a choice from which you may select any or none.

| Separates options.

A.2.1 Pstserv Configuration File

The **pstserv** configuration file is used to configure the system for running pr0svce, the ***Server*** daemon. An example of pstserv.cfg is in the `/etc` subdirectory to the PSTHOME directory. Before you run pr0svce, modify the following parameters to reflect your site requirements, as applicable. In the following syntax, defaults are shown in **bold** text:

[customerid [*n* | **000000**]]
[customername [*custname* | **xxxxx**]]
[license [*xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx* |
000000-000000-000000-000000-000000]]
[rtservername [*servername* | ***localcomputername***]]
tempdir *directory*
datadir *directory*
[datadirclient [**0** | 1]]
[archivedir [*directory* | ***datadir***]]
[archivediridx [*directory* | ***archivedir***]]
[archivebroidx [*directory* | ***archivedir***]]
[maxprocesses [*n* | **48**]]
[tracedays [*n* | **5**]]
[limitaccess [0 | **1**]]
[allowdir *path*]]
[pstlogon [**client** | server]]
[dbaliaslogon [**client** | server]]
[delfileinterval [*n* | **10**]]
[filelogon {client | **local** | server (*userid* { *password* | ? }) }]
[filemode < ALL | RUSR | RGRP | ROTH | WUSR | WGRP |
WOTH | RALL | WALL > | [**SYSTEM**]]
[endpoint [*tcpportnumber* | **1024**]]
pstdir (*name dbmstype dbmsver dbqual connectstring*
{ *dbname* | * *userid* { *password* | ? } })
dbalias (*pstdir name* { *connectstring* | * [*userid* { *password* | ? }] })
[loader ({ (*pstdir dbalias*) | (* *dbmstype*) } *pathtoloader*
excptntblcid)]
[odbcserver [**0** | (1 [*userid* { *password* | ? }])]]
[adminemailnotify (*emailaddress*={ success | information |
warning | **error** | exception } [*n* | **7**] [**0** | 1] [clear])]
[archiveretentionpolicy ({ *hh:mm* | * } { *pstdirectory* | * })]
[centeraavail [**0** | 1]]
[tivoliavail [**0** | 1 (*nodename password*)]]

Keywords

customerid ***Optim*** company identifier.

n	Unique six-digit Company ID provided with ***Optim***.
000000	The ***Optim*** demonstration ID. (Default)

```
customerid 611239
```

customername Customer name.

custname	Company Name provided with Company ID and license key. (Up to 40 characters)
ccccccc	The demonstration name. (Default)

```
customername ccccccc
```

license The license key.

Note: The license key is saved in the registry. This registry entry is replaced if you connect to an ***Optim*** Directory with a more recent key. Therefore, you can remove this keyword after you start pr0svce the first time.

license key	The 5-part license key provided by IBM.
demonstration key	The ***Optim*** demonstration key, shown in the following example. (Default)

```
license 000000-000000-000000-000000-000000
```

rtservername The name of the ***Server*** daemon as declared to all client machines. Processes initiated from a client machine and directed to the ***Server*** are executed if this name matches a name in the Product Configuration File used by the client or, for command line and ODBC processes that explicitly require the ***Server***, the **Server** parameter in pstlocal.cfg.

servername	1- to 15-character name
localcomputer name	The computer name. (Default)

```
rtservername servername
```

tempdir Temporary Directory for temporary work and trace files. If the directory referenced by the keyword does not exist, the Shell script creates it.

```
tempdir      ${PSTHOME}/temp
```

datadir Data Directory for Extract, Compare, Control, Export, and other process files for which a complete path is not provided. If the directory referenced by the keyword does not exist, the shell script creates it.

```
datadir        ${PSTHOME}/data
```

datadirclient Indicator for creating Data subdirectories for client data. Settings are:

0 or blank Do not create client subdirectories. (Default)

1 Create client Data subdirectory as the default Data Directory when a client first connects to the ***Server***.

```
datadirclient  1
```

archivedir Directory for Archive Files for which the process request does not provide a complete path. If the directory does not exist, the shell script creates it. Archive Files are stored in the Data directory (datadir) by default.

```
archivedir  ${PSTHOME}/archive
```

archivediridx Archive Index Directory for Archive Index Files for which a complete path is not provided. If the directory does not exist, the Shell script creates it. Archive Index Files are stored in the Archive Directory (archivedir), or the Data directory (datadir), by default.

```
archivediridx  ${PSTHOME}/archiveidx
```

archivebroidx Archive Browse Index Directory for Archive Browse Index Files for which a complete path is not provided. If the directory referenced by the keyword does not exist, the Shell script creates it. To expedite the retrieval of data, an Archive Browse Index File is created when a user browses archived data and joins tables. By default, Archive Browse Index Files are stored in the Archive Directory (archivedir), or the Data directory (datadir).

```
archivebroidx  ${PSTHOME}/archivebro
```

maxprocesses Maximum number of processes that can run on the ***Server*** simultaneously. When the server reaches the maximum, an error message (**Server too Busy**) is displayed. Specify:

n	A value from 10 to 48. Set the limit according to the capacity of the machine (CPU, disk space, network access speed, memory, etc.), noting that typically, a mirror validation process is created each time a client edits a process request that specifies the ***Server***. Both processes run simultaneously. (For example, if a workstation initiates two processes simultaneously, the ***Server*** executes four processes.)
48	Default setting.

```
maxprocesses 48
```

tracedays Number of days to retain trace files in the temporary work directory. Specify:

n	A value from 2 to 30. Consider storage space limitations when deciding the number of days to retain the files.
5	Default setting.

```
tracedays 5
```

limitaccess Client access to data directories. Settings are:

0 or blank	Client can see all directories on this machine in Browse dialogs.
1	Limit client access to the Temporary (tempdir), Data (datadir), Archive (archivedir), Archive Index (archivediridx), Archive Browse Index (archivebroidx) directories and any directories specified in the allowdir parameter. (Default)

```
limitaccess 0
```

allowdir Option to add a directory to the **limitaccess** list. Use **allowdir** for each additional directory. A valid entry is:

path	A proper directory path (you need not create the directory first)

```
allowdir /dir/subdir...
```

Note: Allowing access to the root directory is equivalent to setting **limitaccess** to 0.

pstlogon The source of DBMS User ID and Password for ***Optim*** Directory access. Valid entries are:

client	User ID and Password for the delegating client (i.e., from the **Server** tab in Personal Options or /PSTDIRUSERID and /PSTDIRPASSWORD from the command line). (Default)
server	User ID and Password provided with **pstdir** keyword.

```
pstlogon client
```

dbaliaslogon The source of DBMS User ID and Password for DB Alias access. Valid entries are:

client	User ID and Password for the delegating client (i.e., from the **Server** tab in Personal Options or /USERID and /PASSWORD from the command line). (Default)
server	User ID and Password provided with **dbalias** keyword.

```
dbaliaslogon client
```

delfileinterval The interval in minutes for deleting Archive Files with an expired retention period after being recalled from secondary media.

n	A value from 0 to 300. Specify 0 to prevent the deletion of recalled files.
10	Default setting.

```
delfileinterval 10
```

filelogon The source of User ID and Password for file access. Valid entries are:

local	User ID and Password used to start pr0svce. (Default)
client	DBMS User ID and Password for the delegating client (i.e., from the **Server** tab in Personal Options or the **server** parameter in pstlocal.cfg).
server ***userid password***	The provided User ID and Password apply for all delegated processes. Specify "?" as the password when a secure password is supplied in a password file. (See **A.4.2 Securing the Configuration Files** for more information.)

Note: If **client** or **server** keyword is used, the pr0svce daemon must be started under root authority.

```
filelogon local
```

filemode Access permissions for Extract, Archive, and Control Files. Use any combination of the following:

ALL	Read and Write permission for all users.
RUSR	Read Permission for User.
RGRP	Read Permission for the group that includes User.
ROTH	Read Permission for all users outside Group.
WUSR	Write Permission for User.
WGRP	Write Permission for the group that includes User.
WOTH	Write Permission for all users outside Group.
RALL	Read permission for all users.
WALL	Write permission for all users.
SYSTEM	The system default, typically Read and Write permission for the User, and Read-Only for Group and Other. (Default)

```
filemode   system
```

- When **filelogon** is **local**, the user account under which the pr0svce daemon is started is User.
- When **filelogon** is **client**, the user that creates a file is User.
- When the **filelogon** value is **server**, the explicitly supplied user account is User.

endpoint The TCP port that pr0svce monitors for RPC connections from clients. Valid settings are:

tcpportnumber	A numeric value from 1024 to 65534.
1024	The default setting.

```
endpoint 6736
```

pstdir

Connection information for an ***Optim*** Directory. Use pstdir for each ***Optim*** Directory that can be accessed on behalf of a client. Note that the ***Optim*** Directory is created from a Windows machine using the **Configuration** program and that connection to the Directory is not verified until required by a client.

name	Name of the ***Optim*** Directory.
dbmstype	Database Management System as DB2, ORACLE, SYBASE or INFORMIX.
dbmsver	DBMS version in the form *n.n*, *n.n.n*, or *n*i, as appropriate to the DBMS.
dbqual	Creator ID, Schema Name, or Owner.
connectstring	Information defined to the DBMS client to connect to the database.
dbname	Name within connection. (Provide name if DBMS is Informix or Sybase ASE and **pstlogon** is **client** or specify '*' if **pstlogon** is **server**.)
userid ***password***	User ID and password for DBMS logon. (Provide this information if **pstlogon** is **server**.) Specify "?" as the password when a secure password is supplied in a password file. (See **A.4.2 Securing the Configuration Files** for more information.) To use OS Authentication for Oracle, specify a forward slash (/) for **userid** and do not specify a password.

```
pstdir OPTIMDIR Oracle 9i APPPROD * USERID ?
pstdir OPTIMDIR DB2 8.1 APPPROD
```

dbalias	DB Alias information. Use dbalias for each DB Alias that the ***Server*** can access on behalf of a client. Note that a DB Alias is created from a Windows machine using the **Configuration** program and the DB Alias information is not verified until a connection is required by a client.
pstdir	Name of the ***Optim*** Directory that includes the DB Alias. A **pstdir** entry for the referenced ***Optim*** Directory is required.

name Name of the DB Alias.

connectstring Information needed by the DBMS to connect to the database (typically, the system name and port ID).

(Enter '*' if the database designated by the DB Alias includes the ***Optim*** Directory.)

userid ***password*** User ID and password for DBMS logon. (Provide this information if **dbaliaslogon** is **server**.)

Specify "?" as the password when a secure password is supplied in a password file. (See **A.4.2 Securing the Configuration Files** for more information.) To use OS Authentication for Oracle, specify a forward slash (/) for **userid** and do not specify a password.

```
dbalias OPTIMDIR DBALIAS * USERID ?
dbalias OPTIMDIR DBALIAS DO805
dbalias OPTIMDIR DBALIAS * USERID PASSWORD
```

loader The location of the DBMS loader for a delegated Load Request. You can identify a loader for a specific ***Optim*** Directory and DB Alias, or you can identify a default loader be used for any DB Alias within a DBMS.

pstdir The Loader is for a specific DB Alias. Enter the name of the ***Optim*** Directory that includes the DB Alias. The ***Optim*** Directory must be referenced in a **pstdir** parameter. This setting requires a ***dbalias*** name.

dbalias The Loader is for a specific DB Alias. Enter the name of the DB Alias. The DB Alias must be referenced in a **dbalias** parameter. This setting requires a ***pstdir*** name.

***** The Loader is the default for a DBMS. You must also provide a value for *dbmstype*.

dbmstype DBMS type. Enter Oracle, Sybase, Informix, or UDB.

pathtoloader Path to the executable loader file.

excptntblcid Default CID for creating an exception table.

```
loader * oracle /opt/oracle/816/bin/sqlldr

loader PSTDIR DBALIAS
   /opt/oracle/816/bin/sqlldr
```

odbcserver Start mode for ODBC Server process. Use this parameter to prevent your having to start the ODBC Server (pr0coms) separately. Note that the pstlocal.cfg file governs the ODBC Server; other parameters and settings in pstserv.cfg do not apply to the ODBC Server.

0 or blank	Do not start the ODBC Server. (Default)
1	Start the ODBC Server using the User ID and Password used to start pr0svce.
userid password	Start the ODBC Server using the specified User ID and password. Specify "?" as the password when a secure password is supplied in a password file. (See **A.4.2 Securing the Configuration Files** for more information.) To use OS Authentication for Oracle, specify a forward slash (/) for **userid** and do not specify a password.

Note: If odbcserver true *userid password* is used, the daemon must be started under root authority.

```
odbcserver false
```

adminemailnotify Option to email "logged" messages reported to the ***Server*** syslog. Provide the email address and severity level. You can also provide options for resending messages.

emailaddress=	The email address to receive the message. If an address contains a space, the entire string for this attribute must be in quotes.
success	Send email notification for all processing messages including **success.** (For example, startup and termination.)
information	Send email notification for **information** or more severe messages.
warning	Send email notification for **warning** or more severe messages.
error	Send email notification for **error** or more severe messages. (Default.)
exception	Send email notification for **exception** messages.

n A number of days, from 0 to 999, after which a message is resent for a persistent error or warning. Specify 0 to resend messages immediately.

0 or blank Do not resend messages. (Default.)

1 Resend a notification for a persistent error or warning.

clear Clear messages to be resent when the ***Server*** starts.

```
adminemailnotify admin@company.net=error 0 false;
admin2@company.net=success 7 true
```

archiveretentionpolicy

Option to scan ***Optim*** Directories for Archive Files with an expired retention period. If the retention period has expired, the ***Server*** will delete the Archive File, Archive Index File, Archive Index Browse File, Archive Directory entry, and Archive Files on backup devices. To delete backup files, you must use the **centeraavail** or **tivoliavail** parameters. NetWorker backups cannot be deleted.

hh:mm The time of day to scan the ***Optim*** Directories. Use 24-hour time format (for example, 1:30 p.m. is 13:30). Midnight is 00:00. Enter '*' to use the default, 00:01.

pstdirectory The ***Optim*** Directories to scan. Separate multiple entries with a comma or space. Enter '*' for all Directories.

```
archiveretentionpolicy 01:00 pstdir1 pstdir2
archiveretentionpolicy 03:00 pstdir3 pstdir4
```

centeraavail Use Centera with the Archive Retention Policy.

0 or blank Do not delete backup files on Centera. (Default.)

1 Delete backup files on Centera.

```
centeraavail true
```

tivoliavail Use Tivoli with the Archive Retention Policy. (To use a Tivoli device, you must install the Tivoli client and API support on the machine where the ***Optim Server*** runs.)

0 or blank Do not delete backup files on Tivoli. (Default.)

1 Delete backup files on Tivoli.

nodename Identifier to access the Tivoli device.

password Password to access the Tivoli device.

A.2.2 Pstlocal Configuration File for the Command Line Utility

Unless a Command Line or ODBC process is specifically directed to a ***Server***, the process is executed locally and the settings in pstserv.cfg do not apply. Use the **pstlocal** configuration file to provide settings for these local processes. An example of pstlocal.cfg is in the `/etc` subdirectory to the PSTHOME directory.

Before using ODBC or the Command Line Utility, modify the following parameters to reflect your requirements, as applicable. In the following syntax, defaults are shown in **bold** text:

[customerid [*n* | **000000**]]
[customername [*name* | **xxxxxxx**]]
[license [*license key* | **000000**]]
tempdir *directory*
datadir *directory*
[archivedir [*directory* | ***datadir***]]
[archivediridx [*directory* | ***archivedir***]]
[archivebroidx [*directory* | ***archivedir***]]
[tracedays [*n* | **5**]]
[server (*name address port userid* { *password* | ? } *domain*)]
[localrtserver *name*]
pstdir (*name dbmstype dbmsver dbqual connectstring*
{ *dbname* | * *userid* { *password* | ? } })
dbalias (*pstdir name* { *connectstring* | * [*userid* { *password* | ? }] })
[loader ({ (*pstdir dbalias*) | (* *dbmstype*) } *pathtoloader*
excptntblcid)]
[allowlocktbls [0 | **1**]]
[cmmaxshuffleretries [*n* | **10**]]
[codepage [*codepgenum* | ***db2default***]]
[dbconnections [**0** | 1 *n* | 1 maximum]]
[formatnumerics [**0** | 1]]
[maxcommitfreq [*n* | **200**]]
[maxextractrows [*n* | **100000**]]
[onlyidxsearch [0 | **1**]]
[orausearraydelete [0 | **1**]]
[reviewdelafterarchive [0 | **1**]]
[reportdir [*directory* | ***unixtempdir***]]
[reportlevel [**0** | *n*]]
[centeraallowaltret [0 | **1**]]
[centeraavail [**0** | 1]]
[centeraretention [**none** | default | interval | infinite]]

[centeradays [**0** | *n*]]
[centerayears [**0** | *n*]]
[networkeravail [**0** | 1]]
[tivoliavail [**0** | 1 [*userid* { *password* | ? }]]]
[rmfixedsegsize [**0** | *n*]]
[rmremsegsize [**10** | *n*]]
[scriptmaxlines [**500** | *n*]]
[scriptprefixout [0 | **1**]]
[scriptshowfullcol [0 | **1 4 4** | 1 *ln rn*]]
[scriptshowfulltbl [0 | **1 4 4** | 1 *ln rn*]]
[scriptwarnmissing [0 | **1**]]
[wormdeviceallowaltret { 0 | **1** }]
[wormdeviceretention { **none** | interval | maximum }]
[wormdevicedays [**0** | *n*]
[wormdeviceyears [**0** | *n*]
[sybaseunchain { **active** | inactive | defaultactive | defaultinactive }]
[uncommittedread { active | **inactive** | defaultactive |
defaultinactive }]

Keywords

customerid Company identifier.

n Unique six-digit Company ID provided with ***Optim***.

000000 The ***Optim*** demonstration ID. (Default)

```
customerid 000000
```

customername Customer name.

name Company Name provided with Company ID and license key. (Up to 40 characters)

xxxxxxx The ***Optim*** demonstration name. (Default)

```
customername xxxxxxx
```

license The ***Optim*** license key.

Note: The license key is saved in the registry. This registry entry is replaced if you connect to an ***Optim*** Directory with a more recent key. Therefore, you can remove this keyword after you start pr0svce the first time.

license key The 5-part license key provided by IBM.

demonstration key The ***Optim*** demonstration key, shown in the following example. (Default)

```
license 000000-000000-000000-000000-000000
```

tempdir Directory for temporary work and trace files.

directory Name of the directory for temporary work and trace files. If this directory does not exist, the shell script creates it.

```
tempdir ${PSTHOME}/temp
```

datadir Directory for Extract, Compare, Control, Export, and other process files for which a complete path is not provided.

directory Name of the directory for Extract, Compare, Control, Export and other process files. If this directory does not exist, the shell script creates it.

```
datadir ${PSTHOME}/data
```

archivedir Directory for Archive Files for which the process request does not provide a complete path. If the directory does not exist, the shell script creates it. Archive Files are stored in the Data directory (datadir) by default.

```
archivedir  ${PSTHOME}/archive
```

archivediridx Archive Index Directory for Archive Index Files for which a complete path is not provided. If the directory does not exist, the Shell script creates it. Archive Index Files are stored in the Archive Directory (archivedir), or the Data directory (datadir), by default.

```
archivediridx  ${PSTHOME}/archiveidx
```

archivebroidx Archive Browse Index Directory for Archive Browse Index Files for which a complete path is not provided. If the directory referenced by the keyword does not exist, the Shell script creates it. To expedite the retrieval of data, an Archive Browse Index File is created when a user browses archived data and joins tables. By default, Archive Browse Index Files are stored in the Archive Directory (archivedir), or the Data directory (datadir).

```
archivebroidx  ${PSTHOME}/archivebro
```

tracedays Number of days to retain trace files in the temporary work directory.

n A value from 2 to 30. The default is 5. Consider storage space limitations when deciding the number of days to retain the files.

```
tracedays 5
```

server Connection for Command Line and ODBC processes that are not executed locally but, instead, are targeted to a ***Server***. You can omit this keyword if, for the targeted ***Server***, file access is limited to a specific Windows user account or the **filelogon** value is **server** or **local**.

name Name of the ***Server***. The target ***Server*** must support a tcp/ip connection.

address The tcp/ip network address for the target ***Server***, in the form 1.1.1.1.

port The numeric tcp/ip port number for the target ***Server***, as a value from 1 to 65534.

userid
password

User ID and password needed to logon to a target ***Server*** set up to receive file logons from "client" or for which the **filelogon** keyword in **pstserv.cfg** is set to **client**.

Specify "?" as the password when a secure password is supplied in a password file. (See **A.4.2 Securing the Configuration Files** for more information.) To use OS Authentication for Oracle, specify a forward slash (/) for **userid** and do not provide a password.

domain

Domain needed to validate User ID and password for access to a ***Server*** on Windows.

Note: If the user is validated as a local user on a ***Server***, enter the ***Server*** name.

```
server optuser 172.16.8.76 1024 rt password
   test.dom
```

localrtserver

If processing from the command line or if using ODBC to access Archive Files created on a ***Server***, you may improve response times by providing the name of the ***Server*** to be considered the Local ***Server*** for ODBC connections. If the ODBC connection or the Archive File ***Server*** name matches the **localrtserver** specification, the connection is made directly to bypass the ***Server*** and speed access to the Archive File. There is no default value.

Note: Do not use **localrtserver** if accessing archived data on a backup device.

name

Name of the ***Server*** to be considered the Local ***Server*** for ODBC connections.

```
localrtserver servername
```

pstdir

Connection information for an ***Optim*** Directory. Use pstdir for each ***Optim*** Directory that can be accessed for processing initiated from the command line. Note that the ***Optim*** Directory is created from a Windows machine using the **Configuration** program and that connection to the Directory is not verified until required by a client.

name

Name of the ***Optim*** Directory.

dbmstype

Database Management System as DB2, ORACLE, SYBASE or INFORMIX.

dbmsver DBMS version in the form *n.n*.

dbqual Creator ID, Schema Name, or Owner.

connectstring Information defined to the DBMS client to connect to the database.

dbname Name within connection. (Provide name if DBMS is Informix or Sybase ASE and **pstlogon** is **client** or specify '*' if **pstlogon** is **server**.)

userid ***password*** User ID and password for DBMS logon. (Provide this information if **pstlogon** is **server**.)

Specify "?" as the password when a secure password is supplied in a password file. (See **A.4.2 Securing the Configuration Files** for more information.) To use OS Authentication for Oracle, specify a forward slash (/) for **userid** and do not specify a password.

```
pstdir ORA806 Oracle 8.0 OPTUSER DO806 * rt
   password
```

dbalias DB Alias information. Use dbalias for each DB Alias that the ***Server*** can access for Command Line and ODBC processes. Note that a DB Aliases is created from a Windows machine using the **Configuration** program and the DB Alias information is not verified until a connection is required in a process.

pstdir Name of the ***Optim*** Directory that includes the DB Alias. A **pstdir** entry for the referenced ***Optim*** Directory is required.

name Name of the DB Alias.

connectstring Information needed by the DBMS to connect to the database (typically, the system name and port ID).

(Enter '*' if the database designated by the DB Alias includes the ***Optim*** Directory.)

userid / ***password*** — User ID and password for DBMS logon. (Provide this information if **dbaliaslogon** is **server**.)

Specify "?" as the password when a secure password is supplied in a password file. (See **A.4.2 Securing the Configuration Files** for more information.) To use OS Authentication for Oracle, specify a forward slash (/) for **userid** and do not specify a password.

```
dbalias ORACLE806 ORACLE806 DO806 rt password
```

loader — The location of the DBMS loader for a command line process. You can specify a loader for a specific ***Optim*** Directory and DB Alias, or specify a default loader be used for any DB Alias within a DBMS.

pstdir — The Loader is for a specific DB Alias. Enter the name of the ***Optim*** Directory that includes the DB Alias. The ***Optim*** Directory must be referenced in a **pstdir** entry. A **pstdir** entry requires a **dbalias** entry.

dbalias — The Loader is for a specific DB Alias. Enter the name of the DB Alias. The DB Alias must be referenced in a **dbalias** entry. A **dbalias** entry requires a **pstdir** entry.

***** — The Loader is the default for a DBMS. You must also provide a value for *dbmstype*.

dbmstype — DBMS type. Enter Oracle, Sybase, Informix, or UDB.

pathtoloader — Path to the executable loader file.

excptntblcid — Default CID for creating an exception table.

```
loader * oracle /opt/oracle/816/bin/sqlldr

loader OPTDIR DBALIAS
   /opt/oracle/816/bin/sqlldr
```

allowlocktbls — Allow users to lock tables.

0 — Do not allow users to lock tables.

1 — Allow users to lock tables. (Default)

```
allowlocktbls 1
```

codepage Code page for System 390 access.

codepgenum Valid code page settings are 37, 273, 277, 278, 280, 284, 285, 297, 500, and 871.

db2default The DB2 default setting. (Default)

```
codepage 871
```

cmmaxshuffleretries Default number of times the Column Map Shuffle Function will refetch a replacement value until a value that does not match the source row is found (a "retry"). The Shuffle Function **retry** parameter overrides this default.

Using a high retry value with columns that contain many duplicate values will increase the processing time. For these columns, it may be best to use a retry value of zero.

n Enter a value from 0-1000. Enter 0 to allow a replacement value to match the source. The default is 10.

```
cmmaxshuffleretries 10
```

dbconnections Number of database connections for Archive, Delete, or Extract Processing. Multiple database connections allow processing of multiple rows concurrently to improve performance when processing large quantities of data. Valid entries are:

0 Use one database connection for processing. (Default)

1 *n* Use the specified number (from 2 to 32) of database connections.

1 maximum Use the maximum number of connections supported by the ***Server***.

```
dbconnections 1 maximum
```

formatnumerics Format of numeric values displayed in process reports.

0 Do not format numbers in process reports (i.e., display as *nnnnnn*). (Default)

1 Format numbers in process reports (i.e., display as *nnn,nnn*).

```
formatnumerics 0
```

maxcommitfreq System-wide commit frequency.

n A number from 1 to 999,999.

200 Default setting.

```
maxcommitfreq 200
```

maxextractrows Maximum number of rows to extract.

n A number from 1 to 999,999,999.

100000 Default setting.

```
maxextractrows 100000
```

onlyidxsearch Use of Archive Indexes in Search and Restore processes. Valid entries are:

0 Search Archive indexes first and native file system, if necessary.

1 Search Archive indexes only. (Default)

```
onlyidxsearch 1
```

orausearraydelete Use the Oracle array delete feature with a Delete Process. When the feature is used, rows not found are listed as deleted in the Delete Process Report. Valid entries are:

0 Do not use Oracle array delete.

1 Use Oracle array delete. (Default)

```
orausearraydelete 1
```

reviewdelafterarchive Allow users to list rows to be deleted after Archive Process.

0 Do not allow users to list rows to be deleted after Archive Process.

1 Allow users to list rows to be deleted after Archive Process. (Default)

```
reviewdelafterarchive 1
```

reportdir Directory or location for saved reports.

directory As you must use a Window workstation to view reports, specify a path accessible from such a workstation.

unixtempdir The UNIX or Linux temporary directory. (Default)

```
reportdir /users/RTuser/DDRIVE/OUTDIR/REPORTS
```

reportlevel Maximum number of reports to retain for each type of process (e.g., Extract Processes, Archive Processes). Valid entry is 0 - 200. A value of 0 (default) disables the report retention feature.

0 Do not retain reports. (Default)

n The number of reports retained for a particular process (up to 200) Once the number of retained reports equals this amount, the oldest report is deleted as the current report is saved.

```
reportlevel 0
```

centeraallowaltret Indicator for minimum Centera retention settings.

0 Use the Centera default. Any Storage Profile or **centeraretention** settings for retention will cause the process to fail.

1 Use **centeraretention** settings or overriding Storage Profile settings for minimum Centera retention. (Default) If **centeraavail** is 0, the Archive Process will fail.

```
centeraallowaltret 1
```

centeraavail Indicator for the use of a Centera device.

0 Centera device is not used. (Default)

1 Centera device is available for use. This setting is required in order to copy an Archive File to a Centera device or process such a file.

```
centeraavail 0
```

centeraretention Default minimum retention setting for Archive Files copied to Centera.

none No minimum retention period. (Default)

default The Centera default applies.

interval Use any **centeradays** and **centerayears** settings or overriding Storage Profile settings for minimum Centera retention.

infinite Retain the file on Centera forever; the file cannot be deleted.

```
centeraretention none
```

centeradays The number of days to retain an Archive File copied to Centera. This value and the **centerayears** value determine the retention period when the **centeraretention** parameter or overriding Storage Profile setting indicates an interval for Centera File retention.

0 Default. The file can be deleted from Centera at any time.

n Number of days (up to 18300) to retain the file.

```
centeradays n
```

centerayears The number of years to retain an Archive File copied to Centera. This value and the **centeradays** value determine the retention period when the **centeraretention** parameter or overriding Storage Profile setting indicates an interval for Centera File retention.

0 Default. The file can be deleted from Centera at any time.

n Number of years (up to 100) to retain the file.

```
centerayears n
```

networkeravail Indicator for the use of a NetWorker system.

0 NetWorker is not used. (Default)

1 NetWorker is available for use. This setting is required in order to copy an Archive File to NetWorker or to process such a file.

```
networkeravail 0
```

tivoliavail Indicator for the use of a Tivoli device.

Note: To use a Tivoli device, you must install the Tivoli client and API support on the machine where the ***Optim Server*** runs.

0 Tivoli is not used. (Default)

1 Tivoli is available for use. This setting is required in order to copy an Archive File to Tivoli or to process such a file.

userid password Tivoli is available for use with the specified User ID and password. This setting is required in order to copy an Archive File to Tivoli or to process such a file.

Note: If this setting is used, pr0svce must be started under root authority. See **A.4.1 Securing the Products**.

```
tivoliavail 1
```

rmfixedsegsize The default maximum segment size for Archive Files on fixed drive (i.e., hard disk).

0 Fixed drive software determines default segment size. (Default)

n Size in megabytes (up to 9999 MB).

```
rmfixedsegsize 0
```

rmremsegsize The default maximum segment size (in megabytes) for Archive Files on a removable device (e.g., floppy disk, zip drive).

10 Default

n Size in megabytes (up to 9999 MB).

```
rmremsegsize 10
```

scriptmaxlines Maximum number of lines in a Column Map Procedure that are included in the Process Report.

500 Include up to 500 lines. (Default)

n Maximum number of lines to include (up to 9999 lines).

```
scriptmaxlines 500
```

scriptprefixout Option for Column Map Procedure name in Process Report.

0 Do not include name.

1 Include Column Map Procedure name. (Default) If a Local Column Map Procedure is used in process, a name is generated in the form *tablename.columename.n* to be included in the report. Use **scriptshowfullcol** and **scriptshowfulltbl** to format the generated name.

```
scriptprefixout 1
```

scriptshowfullcol Format for column name used to generate name for local Column Map Procedure.

0 Use full column name.

1 4 4 Use first 4 characters and last 4 characters in column name. (Default)

1 *ln rn* Use indicated number of characters from beginning (*ln*) and end (*rn*) of column name.

```
scriptshowfullcol 1 3 3
```

scriptshowfulltbl Format for table name used to generate name for local Column Map Procedure.

0 Use full table name.

1 4 4 Use first 4 characters and last 4 characters in table name. (Default)

1 *ln rn* Use indicated number of characters from beginning (*ln*) and end (*rn*) of table name.

```
scriptshowfulltbl 1 6 6
```

scriptwarnmissing Report option for missing Column Map Procedures.

0 Exclude warning of missing Column Map Procedure.

1 Include warning of missing Column Map Procedure. (Default)

```
scriptwarnmissing 1
```

wormdeviceallowaltret

Indicator for minimum WORM device retention settings. Indicates whether users can override configuration specifications for a WORM device using a Storage Profile.

0 Use the WORM device default. Any Storage Profile or **wormdeviceretention** settings for retention will cause the process to fail.

1 Use **wormdeviceretention** settings or overriding Storage Profile settings for minimum WORM device retention. (Default)

```
wormdeviceallowaltret 1
```

wormdeviceretention Default minimum retention setting for Archive Files copied to a WORM device.

none No minimum retention period. (Default)

interval Use any **wormdevicedays** and **wormdeviceyears** settings or overriding Storage Profile settings for minimum WORM device retention. The retention interval cannot exceed the WORM device maximum date of 01/17/2071.

maximum The WORM device maximum retention date, 01/17/2071, applies.

```
wormdeviceretention none
```

wormdevicedays The number of days to retain an Archive File copied to a WORM device. This value and the **wormdeviceyears** value determine the retention period when the **wormdeviceretention** parameter or overriding Storage Profile setting indicates an interval for WORM device file retention.

0 Default. The file can be deleted from the WORM device at any time.

n Number of days (up to 999) to retain the file.

```
wormdevicedays 60
```

wormdeviceyears The number of years to retain an Archive File copied to a WORM device. This value and the **wormdevicedays** value determine the retention period when the **wormdeviceretention** parameter or overriding Storage Profile setting indicates an interval for WORM device file retention.

0 Default. The file can be deleted from the WORM device at any time.

n Number of years to retain the file.

```
wormdeviceyears 20
```

sybaseunchain ***Optim*** normally runs in chained mode. However the connection must be in unchained mode to accommodate a Sybase ASE stored procedure that runs in unchained mode, if the stored procedure will be triggered in a command line process to Insert, Restore or Delete Sybase ASE data.

- **active** Processes must run in unchained mode.
- **inactive** Processes must run in normal (chained) mode. (Default)
- **defaultactive** The **Run in Unchained Mode** check box in Personal Options is available and selected, by default. Insert, Restore, and Delete Processes run in unchained mode unless the **Run in Unchained Mode** check box in Personal Options is cleared.
- **defaultinactive** The **Run in Unchained Mode** check box in Personal Options is available and cleared, by default. Insert, Restore, and Delete Processes run in normal mode unless the **Run in Unchained Mode** check box in Personal Options is selected.

```
sybaseunchain active
```

uncommittedread Option to enable extracting of uncommitted rows from the database during an Archive or Extract Process. You can extract uncommitted rows from specific tables in the Access Definition or all tables. Selecting this option for tables with known performance problems may increase the speed of your Archive or Extract Processes.

- **active** Automatically extract uncommitted rows from each table in the Access Definition during all Archive or Extract Processes.
- **inactive** Automatically extract only committed rows from each table in the Access Definition during all Archive or Extract Processes. (Default.)
- **defaultactive** The **Uncommitted Read** option on the **Access Definition Editor** is available and selected by default. Uncommitted rows are extracted unless this option is cleared.

defaultinactive The **Uncommitted Read** option on the **Access Definition Editor** is available and cleared by default. Uncommitted rows are not extracted unless this option is selected.

```
uncommittedread inactive
```

A.2.3 RTSETENV Shell Script

This file is the script designed to be included in a user ".profile" or ".login" script to define the operating environment for the ***Server***. The RTSETENV script sets up the ***Server*** daemon or command line environment on login. A sample is in the PSTHOME directory.

The UNIX operating environment requires certain environment variables to create default settings, as applicable:

PSTHOME=*directory*
[PSTINFO=[*directory*]]
[ORACLE_HOME=[*directory*]]
[TNS_ADMIN=[*directory*]]
[RTORACLELIB=[*directory*]]
[DB2CODEPAGE=*n*]
[RTDB2PROFILE=[*directory*]]
[SYBASE=[*directory*]]
[RTSYBASELIB=[*directory*]]
[INFORMIXDIR=[*directory*]]
[INFORMIXSERVER=*server*]
[INFORMIXSQLHOSTS=[*directory*]]

Environment Variables

PSTHOME — The location of ***Optim***.

```
PSTHOME=/opt/IBM/Optim
```

PSTINFO — The location of process information files for ***Optim*** (all installations). If this environment variable is not set, it defaults to the following:

```
PSTINFO=/var/tmp/rt4s
```

Set this variable if you do not have access to /var/tmp, or if you want to direct process information to another location.

Note: All installations of ***Optim*** must point to the same location.

ORACLE_HOME — The location of Oracle.

```
ORACLE_HOME=/opt/oracle
```

TNS_ADMIN — The location of file tnsnames.ora.

```
TNS_ADMIN=/opt/oracle
```

RTORACLELIB	The location of the Oracle API shared objects. `RTORACLELIB=${ORACLE_HOME}/lib`
DB2CODEPAGE	The code page for DB2. `DB2CODEPAGE=1252`
RTDB2PROFILE	The location of the DB2 environment script, db2profile. `RTDB2PROFILE=/opt/db2ad81/sqllib`
SYBASE	The location of Sybase ASE. `SYBASE=/opt/sybase`
RTSYBASELIB	The location of the Sybase ASE API shared objects. `SYBASE=/opt/sybase/syb12/OCS-12_0/lib`
INFORMIXDIR	The location of Informix. `INFORMIXDIR=/opt/informix`
INFORMIXSERVER	The name of the Informix server when the product was configured.
INFORMIXSQLHOSTS	The location of Informix SQLHOSTS. `INFORMIXSQLHOSTS=${INFORMIXDIR} / sqlhosts`

A.2.4 RTSERVER Shell Script

The RTSERVER shell script is located in the `/sbin` directory that is subordinate to the ***Optim*** installation directory. This shell script contains commands that may be useful to manipulate the ***Server*** process. Generally, the RTSERVER script does not need modification.

You must change the script, however, if the ***Server*** is installed in a directory other than the default directory, /opt/IBM/Optim, or if the ***Server*** will be run under a user account other than root. The script contains areas that allow you to modify the following environment variables:

- Set PSTHOME=${PSTHOME:*directory*/rt} to define the directory containing the ***Server***.

- Set PSTUSER=${PSTUSER:*user*} to identify a user other than root.

Arguments

RTSERVER arguments define the operation to be performed, as follows:

rtserver start	Start the ***Server*** in the background. The stdout and stderr produced by the ***Server*** are written to a file named pr0svce.out, which can be found in the temp directory that is subordinate to the ***Optim*** installation directory.
rtserver stop	Stop a running ***Server*** instance. The ***Server*** stops after processes are complete.
rtserver kill	Kill a running ***Server*** instance. The ***Server*** stops abruptly, without regard to running processes.
rtserver update	Re-read the Pstserv configuration file after processes have completed. Use this command to effect changes to the configuration file without restarting the ***Server***.
rtserver list	List all processes running on the ***Server***. The list includes the PID of the process, the name of the computer delegating the process, the ***Optim*** Directory that is active for the process, the type of process (archive, extract, etc.), the name of the process request, the time the process started, and period for which it has been running.
rtserver verify server	Verify settings in the pstserv configuration file, used to configure the system for running the ***Server***.
rtserver verify local	Verify the settings in the pstlocal configuration file, which provides settings for local operation, using the command line or ODBC.

A.2.5 RT4S Shell Script

The RT4S shell script is used to start or stop the ***Server*** from init(1) processing, and should be executed as part of the system boot procedure only. Generally, the RT4S script does not need modification.

You must change the script, however, if the ***Server*** is installed in a directory other than the default directory, /opt/IBM/Optim/rt, or if the ***Server*** will be run under a user account other than root. The script contains areas that allow you to modify the following environment variables:

- Set PSTHOME=${PSTHOME: *directory*/rt} to define the directory containing the ***Server***.
- Set PSTUSER=${PSTUSER:*user*} to identify a user other than root.

Symbolic Links

A symbolic link allows a filename in one directory to point to a file in another directory. To start up and shut down the ***Server*** as part of init processing, you must create symbolic links to the RT4S script in the following directories:

- rc2.d, where 2 is the run level for startup
- rc1.d, where 1 is the run level for shutdown

The location of the rc2.d and rc1.d directories is platform-specific:

- Under Solaris and Linux, the location is `/etc`.
- Under HP-UX, the location is `/sbin`.
- Under AIX, the location is `/etc/rc.d`.

Use the **link** command to create symbolic links, as follows:
`ln -s actualfile linkname`.

actualfile	File to which a symbolic link points. In this case, specify RT4S.
linkname	Name of a symbolic link used to point to a file. In this case, point links named S99RT4S and K07RT4S to RT4S.

Solaris or Linux

To start up and shut down the ***Server*** during Solaris or Linux init processing, create symbolic links to the RT4S script in directories `/etc/rc2.d` and `/etc/rc1.d`, as follows:

1. Log in as the root user.
2. From the console, enter the following commands:
   - ln -s /opt/IBM/Optim/rt/sbin/rt4s /etc/rc2.d/S99rt4s
   - ln -s /opt/IBM/Optim/rt/sbin/rt4s /etc/rc1.d/K07rt4s

HP-UX

To start up and shut down the ***Server*** during HP-UX init processing, create symbolic links to the RT4S script in directories `/sbin/rc2.d` and `/sbin/rc1.d`, as follows:

1. Log in as the root user.
2. From the console, enter the following commands:
   - ln -s /opt/IBM/Optim/rt/sbin/rt4s /sbin/rc2.d/S99rt4s
   - ln -s /opt/IBM/Optim/rt/sbin/rt4s /sbin/rc1.d/K07rt4s

AIX

To start up and shut down the ***Server*** during AIX init processing, create symbolic links to the RT4S script in directories `/etc/rc.d/rc2.d` and `/etc/rc.d/rc1.d`, as follows:

1. Log in as the root user.
2. From the console, enter the following commands:
   - ln -s /opt/IBM/Optim/rt/sbin/rt4s /etc/rc.d/rc2.d/S99rt4s
   - ln -s /opt/IBM/Optim/rt/sbin/rt4s /etc/rc.d/rc1.d/K07rt4s

A.2.6 LOCALE.CONF Conversion File

The LOCALE.CONF file provides locale conversion information between platforms. An example of LOCALE.CONF is in the `/etc` subdirectory to the PSTHOME directory.

Use the area at the end of this file to provide additional locale conversion information between or within platforms. Specify locale conversion information using the following format:

LocaleA LocaleB

A.3 Maintenance and Performance

A.3.1 Commands

The following commands can generally be used to start, stop, and maintain pr0svce, the ***Server*** daemon. These commands are unique to the ***Server*** under UNIX.

Note: Only one command line argument can be presented at a time. An argument must be preceded by a dash (-) or a slash (/).

pr0svce -h Display Help.

pr0svce -s [*id1*] Shut down pr0svce after last client disconnects.

id1 Process ID, User ID, or endpoint to identify pr0svce. Leave blank to shut down daemons started under the logged on account.

pr0svce -u [*id1*] Reload configuration file for pr0svce.

id1 Process ID, User ID, or endpoint to identify pr0svce. Leave blank to reload for daemons started under the logged on account.

pr0svce -d [*id1*] Display all instances of pr0svce in the system. This command can be run under root or any user account to determine whether pr0svce is running.

id1 Process ID, User ID, or endpoint to identify pr0svce. Leave blank to display all daemons for all users.

pr0svce -l [*id1*] List active processes and clients connected to pr0svce. The PID for each client is displayed, and can be referenced in the -c (cancel client) command.

id1 Process ID, User ID, or endpoint to identify pr0svce. Leave blank to list for all daemons for all users.

pr0svce -k [*id1*]

Shut down pr0svce without waiting for clients to disconnect.

Use this command only when the normal shutdown (-s) is inoperative. Open datasets (including the trace file) are truncated to the last written buffer and each client SVER process must be identified and killed individually.

id1	Process ID, User ID, or endpoint to identify pr0svce. Leave blank to shutdown all daemons started under the logged on account.

pr0svce -daemon

Start pr0svce as a foreground process.

To run pr0svce as a background process, use:

```
nohup pr0svce -daemon
   >outfilename 2>&1 &
```

This command causes any hang-up signals to be ignored, and directs standard output (stdout) and standard error (stderr) streams to *outfilename*, appending stderr to stdout.

pr0svce -c { *clientid* | ALL } | [*id1*]

Cancel client(s) processes.

clientid	Specify client name, or client process ID, or the word ALL.
id1	Provide process ID, User ID, or endpoint to identify pr0svce or leave blank to cancel clients for all daemons started under the logged on account.

pr0svce -v *configuration file name*

Validate the contents of a configuration file and exits.

configuration file name	Valid configuration file name. If you do not provide a configuration file name, the normal server is validated.

A.3.2 Temporary Files

You must shut down all ***Optim*** processes before deleting the following files in the /tmp directory:

- Directories with names beginning with “Mw_” or files, whether open or closed, within those directories
- Files, whether open or closed, with names beginning with “Mw”
- Files, whether open or closed, with names beginning with “regss”

Optim requires that these files not be deleted while any ***Optim*** process (for example, pr0svce, pr0cmnd, etc.) is running. Even though some of these files are of type ‘s,’ they may be safely deleted after all ***Optim*** processes are shut down. In addition, you must shut down all ***Optim*** processes before killing watchdog, mwrpcss, or regss, and before stopping mwadm.

Optim writes log and error files to the /tmp/softech directory during installation. These files may contain diagnostic information should the setup program fail. Once the installation has been deemed successful, the /tmp/softech directory can be safely deleted.

A.4 Securing the Products and Configuration Files

This section provides guidelines for obtaining the most protection on UNIX systems when installing and executing ***Optim***. This section also describes the program (pr0pass) used to encrypt passwords for parameters in the configuration files.

A.4.1 Securing the Products

Installation

UNIX allows you to restrict read, write, or execute permission to a user, members of a group, or members of any other group. Thus, to "fence" ***Optim***, an administrator might:

- Create a group for user accounts with permission to execute ***Optim***.
- Within that group, create a user account to be the designated "owner" of ***Optim***, with full access rights.
- Install ***Optim*** while logged on as the owner and create the install directory as a subdirectory of the home directory.

Under this scenario, typical system defaults for the file creation mask allow only the owner to write to the install directory, the subdirectories, and files within them, while user accounts within the group can execute ***Optim*** and can write to the temp and data subdirectories that hold data from processing. Creating the install directory in the home directory prevents users outside the group from executing ***Optim***.

An alternative method to prevent users outside the group from executing the software is to change permissions by using the chmod command, as follows:

```
chmod o-rwx <install--directory>
```

User Accounts

Before any processing occurs, you should establish all user accounts. If you change user accounts after processes have run, the ability of processes to access files produced in earlier processing may be affected. For example, a Restore Process that uses Centera or NetWorker as the user id in effect when the file is recalled from a backup device and when the recalled file is deleted from disk after the specified retention period. Use the following information to help determine which user ids to specify for each parameter.

The user account under which the pr0svce daemon is started (i.e., the account that is logged on when pr0svce is started) must have write access to the ***Optim*** temporary directory, and read access to pstserv.cfg.

As you establish additional user accounts, keep in mind the following parameter settings in the configuration files, which affect the credentials under which the pr0svce daemon runs, as well as the credentials presented to run a process and to access files during a process.

filelogon The filelogon parameter indicates the source of the credentials for processes.

Unless you override the normal umask behavior using the filemode configuration parameter, output files (Extract Files, Archive Files, Control Files) inherit the standard file privileges of the processing user account. Thus, if you use the **filelogon client** parameter, a process may be unable to access files not created under its own user account and can open files only according to the file permissions, which include access to networked files.

If, however, you use the **filelogon local** parameter, or the **filelogon server** *userid password* parameter, any process can access a file created by any other process and any accessed directories must be writable to the processing user account.

Valid settings are:

local The process runs under the user account used to start the pr0svce daemon.

client The process runs under the user account specified on the **Personal Options Server** tab for the initiating Windows client or the overriding **server** credentials specified in pstlocal.cfg.

server *userid password* The process runs under the credentials provided with the **server** parameter.

Note: **client** or **server** settings require root authorization for the user account used to start the pr0svce daemon; a local setting does not.

odbcserver The odbcserver parameter provides the credentials presented for physical access to Archive Files. Archive Files inherit the standard file privileges of the user account for the Archive Process under which it was created (based on the **filelogon** and **filemode** configuration parameters).

Valid settings are:

1	Present the credentials used to start the pr0svce daemon for physical access to Archive Files.
1 *userid password*	Present the credentials provided with the **odbcserver** parameter for physical access to Archive Files.
0	Do not use the ODBC Server.

Note: A **1** *userid password* setting requires root authorization for the user account used to start the pr0svce daemon.

tivoliavail *userid password* The tivoliavail parameter provides the credentials for physical access to the Tivoli resources. The **filelogon** parameter establishes credentials presented for access to the Archive Files managed by Tivoli.

Valid settings are:

1	Present the credentials used to start the pr0svce daemon for physical access to Tivoli resources.
1 *userid password*	Present the credentials provided with the **odbcserver** parameter for physical access to Tivoli resources.
0	Do not use Tivoli resources.

Note: A **1** *userid password* setting requires root authorization for the user account used to start the pr0svce daemon.

webserver The webserver parameter applies to ***Optim*** **Amdocs CRM Solution** only. For details, see your Tomcat documentation.

Valid settings are:

1	Present the credentials used to start the pr0svce daemon for webserver access to Archive Files.
1 *userid password*	Present the credentials provided with the **odbcserver** parameter for webserver access to Archive Files.
0	Do not use webserver access.

Note: A **1** *userid password* setting requires root authorization for the user account used to start the pr0svce daemon.

When setting up user accounts and file permissions, note that both pr0svce and the user account running pr0svce must be able to access the file that keeps information on active daemons in order to perform an action against pr0svce (for example, to shutdown or delete pr0svce). This file is maintained in the directory designated by the PSTINFO environment variable. (See **A.2.3 RTSETENV Shell Script** for more information regarding the PSTINFO environment variable.)

Execution

If the configuration file includes "filelogon local" or odbcserver, tivoliavail, or webserver parameters without explicit credentials, the process assumes the authority of the user account used to start pr0svce. Thus, if you start pr0svce from the root user, the request will run under root credentials. If you start pr0svce under a user account in the group, the request will run under the credentials for the user account.

As a general rule, you will want to avoid running pr0svce under root authority. However, as noted earlier, you must run the pr0svce daemon under root authority when certain parameters in pstserv.cfg or pstlocal.cfg (i.e., the configuration file) are set. The parameters and settings that require root authority are:

- filelogon client
- filelogon server *userid password*
- odbcserver true *userid password*
- tivoliavail true *userid password*
- webserver true *userid password* (for ***Optim-AMD*** users only)

Before running a process for which one or more of these settings apply, pr0svce validates the incoming user account and password. The process is then run under the credentials supplied in the configuration file. If pr0svce must run a process under root authority, it is advisable to

include the "filelogon server *userid password*" (rather than "filelogon client" or "filelogon local") and the limitaccess parameters in the configuration file to protect your system from processing that, because it uses root credentials, has access to all files on the system.

A.4.2 Securing the Configuration Files

If the administrator has set up file permissions as described in **A.4.1 Securing the Products**, only the owner, members of the group that includes the owner, and the root user can view (read) the configuration files, and only the owner or the root user can update (write) the configuration files.

The user account used to start pr0svce must have read access to the pstserv.cfg file, while the Command Line Utility (pr0cmnd) and the ODBC Server (pr0coms) must have read access to the pstlocal.cfg file. (For details about the configuration files, refer to **A.2.1 Pstserv Configuration File** and **A.2.2 Pstlocal Configuration File for the Command Line Utility**.)

Password File

Parameters in both configuration files may include system user ids (i.e., filelogon, odbcserver, webserver, server, and tivoliavail), DBMS logons (i.e., pstdir and dbalias) with passwords. To secure passwords for configuration parameters, you can use an encrypted password file, separate from the configuration files. The pr0pass program maintains the password file, encrypting passwords for parameters in the configuration files.

By default, the password file is installed in the `/etc/pstpass` subdirectory to the PSTHOME directory. However, you can override the location and name of the file by providing the full path and file name in PSTPASS, an environment variable. (Refer to **A.2.3 RTSETENV Shell Script** for a description of the PSTPASS environment variable.) Users that can start pr0svce or execute pr0cmnd or pr0coms must have permission to read the password file and users that use pr0pass must be able to write to the password file.

Note: Do not move the password file to another system; to do so will corrupt the file.

To use encrypted passwords:

- Execute pr0pass from the Command Line to add the passwords. You must be logged on to the Install directory as the owner, as a user within the fenced group, or as the root user.
- Within the configuration files, specify a question mark (?) for the password to retrieve the password from the password file.

Commands

The following command line actions are available to help you edit an encrypted password file.

pr0pass -l

List the type, name, and user id for passwords in the file.

pr0pass -h
or **-?**

Display the help for the pr0pass program.

pr0pass -a
type name userid password

Add a password entry. The password is encrypted until passed to the DBMS or system for validation.

type A valid password type:

- filelogon
- odbcserver
- webserver
- server
- tivoliavail
- pstdir
- dbalias
- user

Note: "User" is not a parameter in a configuration file; it refers to any system user id. Specify the "user" parameter type for any parameter referring to a system user account.

name The name of the configuration file parameter.

- If *type* is pstdir, the default "%" indicates any ***Optim*** Directory.
- If *type* is dbalias, use the form *pstdir*:*dbalias*. The default "%" indicates any ***Optim*** Directory or DB Alias, as in %:%, *pstdir*:%, or %:*dbalias*.
- Names not associated with other types are system; use "%" for the name value to prevent an error.

userid The user id used to verify that the password matches the parameter name. To protect changes to the password file or the configuration file, the two keywords must match.

password The password that matches the user id.

Note: If you do not enter a password on the Command Line, pr0pass prompts for one.

pr0pass -d *type name userid*

Delete a password entry.

type A valid password type:

- filelogon
- odbcserver
- webserver
- server
- tivoliavail
- pstdir
- dbalias
- user

name The name of the configuration file parameter.

Note: Use the wildcard character "%" as described for adding a password entry.

userid The user ID used to verify that the password matches the parameter name. To protect changes to the password file or the configuration file, the two keywords must match.

Examples

The following examples demonstrate using the Add command for the pr0pass program and indicating encrypted passwords in the configuration file.

1. To encode the password for the ***Optim*** Directory, PSTDIR1, create a password, as follows:

   ```
   pr0pass -a pstdir pstdir1 myuserid mypassword
   ```

   In the configuration file for PSTDIR1, specify the password as a question mark (?):

   ```
   pstdir pstdir1 Oracle 8.0 schema connectstr *
      myuserid ?
   ```

2. To encode the password for the DBALIAS, specify both the ***Optim*** Directory to which it belongs and the DB Alias name:

```
pr0pass -a dbalias pstdir1:dbalias1 myuserid
   mypassword
```

   And in the configuration file, specify:

```
dbalias pstdir1 dbalias1 connectstr myuserid ?
```

3. To encode a single password for a specific user account to access any ***Optim*** Directory or DB Alias, use a percent sign (%) for the *name*. For example:

```
pr0pass -a pstdir % myuserid mypassword
pr0pass -a dbalias %:% myuserid mypassword
```

   This example would provide a password for the following parameters in the configuration file:

```
pstdir pstdir1 Oracle 8.0 schema connectstr *
   myuserid ?
pstdir pstdir2 Oracle 8.0 schema connectstr *
   myuserid ?
dbalias pstdir1 dbalias1 connectstr myuserid ?
dbalias pstdir1 dbalias2 connectstr myuserid ?
dbalias pstdir2 dbalias3 connectstr myuserid ?
```

   But would not provide a password for these parameters in the configuration file:

```
pstdir pstdir3 Oracle 8.0 schema connectstr *
   otherid ?
dbalias pstdir1 dbalias3 connectstr * otherid ?
```

Protecting the Password File

By default, the owner and the root user have write access to the password file and can use the commands, `pr0pass -a` or `pr0pass -d`, to update the password file.

To allow other members of the group to update the password file, you must use the chmod command to change permissions to the password file. For example, the following command adds write permission to the group for the pstpass file.

```
chmod  g+w  <installdir>/etc/pstpass
```

This allows members of the group to maintain passwords for their accounts. However, if members of the group other than the owner have write permission, anyone in the group can delete a password or the

password file, at the risk of disabling the product or requiring reentry of all affected passwords.

Protecting the Configuration Files

It is recommended that you allow only the owner or the root user to update the configuration files. Maintenance of the configuration file does not require knowledge of the actual passwords if group members are allowed to update the password file since the character "?" can be specified for the passwords.

Note: Group members who can modify the configuration file would be able to obtain additional privileges to the ***Optim*** Directory or DB Alias, or execute the ODBC Server or client processes under any identifier.

A.5 The Optim Exit in UNIX

Optim includes a mechanism that allows you to use a custom exit to apply an additional layer of security to ***Optim***, beyond the extensive security already included in the product, to meet any security requirements mandated by your company or government regulations. This additional security layer is accomplished through a client-supplied exit that identifies who can use ***Optim*** and which executables each user can run.

Client-supplied exits are called **user-supplied exits** in ***Optim*** to differentiate them from the **default exit** supplied with ***Optim***. The ***Optim*** default exit allows all requests by all users, within the security limitations defined for each user or user group via the security functionality included in ***Optim***.

The default exit is intended for clients who do not need to use a user-supplied exit, although it may also be used as a temporary solution while you create your own, customized exit. If you use the default exit, ***Optim*** user security will function as it did prior to release 6.5.

If you implement a user-supplied exit, that exit will augment the extensive security functionality already included in ***Optim***.

Note: A user-supplied exit may also be used do other functions, such as manage user accounts, monitor user activity, force inactive sessions to timeout, audit product use, and override user authorization credentials.

Regardless of which exit you use (i.e., the default exit or your own exit), you must "sign" that exit before you can use ***Optim***. After the exit is assigned, ***Optim*** will invoke that exit at initialization and call it at various "exit points" points in the program to determine whether ***Optim*** should continue with what it was about to do. An exit point is a point within a program at which an exit routine can take control to do some external function. The exit allows you to:

- See what is being done by a given user at various points in a program's logic,
- Ensure that the user's request meets your company standards, and
- Change the request, if needed, to pass your company standards or forbid the request altogether.

Optim will call the exit at each exit point to verify that the user's request meets your company standards, such as verifying that the user has permission to run a given executable. The first exit point occurs when the user launches ***Optim***. If you use the exit to provide external security, that exit point determines whether the user has permission to access the product. If the user has the appropriate permissions, the user can continue; if not, ***Optim*** will terminate the user's session after displaying an appropriate error message. (See the **Optim Initialization Exit Programmer's Guide** for a list of a complete list of the ***Optim*** exit points.)

Beginning with ***Optim*** release 6.5, a "signed" exit must exist to use ***Optim***, whether the exit is the ***Optim*** default exit or a user-supplied exit. To sign an exit, you must specify the "company credentials" supplied to your organization when you received ***Optim***. Your company credentials consist of your ***Optim***-supplied company ID, Name, and Password. The ***Optim*** setup process will automatically request these credentials during installation, so you can sign an exit.

Note: If you have write access to the ***Optim*** bin directory and you have the appropriate company credentials, you can change from one exit to another at any time following installation by signing a new exit. You can change from using the default exit to a user-supplied exit (or vice versa), or you can change from one user-supplied exit to another. (If you are switching to user-supplied exit, you must compile, link, and copy that exit to the bin directory before you can sign it.)

In a UNIX environment, you can only sign the default exit during installation (i.e., during the ***Optim*** **Setup** program). If you want to sign a user-supplied exit, you must run an **opmusign** script file following installation. (Another script file is available to revert to the default exit from a user-supplied exit, if needed.) See **A.5.3 Signing an Exit in UNIX** on page 406 for more information.

The ***Optim*** default exit is delivered unsigned to ensure:

- it is signed by a user with the appropriate company credentials, and
- the person signing the default exit is authorized to make the decision to use that exit, as opposed to a user-supplied exit. This is important because the default exit returns a "continue" code at every exit point. Thus, if the default exit was delivered signed, it would bypass any security checks and additional functionality included your user-supplied exit (assuming you already created one).

A.5.1 Writing Your Own Exit

If you want to employ the additional functionality available via a user-supplied exit, you must write your own exit. To write an exit, you must do the following:

1. Determine what you want the exit to do.
2. Determine which ***Optim*** *exit points* that call your exit are suitable for what you want to do.
3. Write the appropriate code to respond to those exit points within your user-supplied exit.

After you create an exit, you must compile, link, and copy the exit to the bin directory in which ***Optim*** is installed, before you can sign it. The same is true when you modify an exit. If a signed exit does not exist, you cannot use ***Optim***. (See the **Optim Initialization Exit Programmer's Guide** for more information on creating a user-supplied exit.)

A.5.2 Prerequisites to Signing a User-Supplied Exit

If you want to use your own, user-supplied exit, the following requirements apply:

- The exit load linked module name must be appropriate for your platform, as shown below:

Platform	Linked Module File Name
Windows	**opmexit.dll**
AIX, Solaris, Linux	**libopmexit.so**
HPUX	**libopmexit.sl**

- You must copy the exit file to the **bin** directory *before* you run the **opmusign** script in UNIX. (The **opmusign** script is used to sign a *user-specified* exit, while the **opmdsign** script is used to sign the *default* ***Optim*** exit.)
- The exit file must exist in the **bin** directory and be signed on *every* ***Optim*** installation. Thus, each time you install ***Optim*** in a directory,

a signed exit must exist in the bin directory. (If you install a new version of ***Optim*** over a previous version, you have to re-copy your exit into the **bin** directory and resign it, or sign the default exit.)

Signing Required After Each Install

Unlike the ***Optim*** Security feature, which you must initialize once per ***Optim*** Directory, you must sign an exit *each time you install* ***Optim*** on a machine. Moreover, when you upgrade to a new ***Optim*** release, you must sign a valid exit for each ***Optim*** installation, before you can use ***Optim***. The same is true if you reinstall ***Optim***.

Anytime you replace a signed exit executable (i.e., opmexit.dll, libopmexit.so, or libopmexit.sl) with another version of that exit, you must sign the updated exit to use ***Optim***. This is true, even if the executable was previously signed (e.g., in another installation or copied from a backup of a signed exit).

A.5.3 Signing an Exit in UNIX

Unlike in Windows, UNIX does not include a **Configuration** program to sign an exit. There are, however, three ways to sign the *default* exit in UNIX, and two ways to sign a *user-supplied* exit in UNIX.

The three ways to sign the *default* exit in UNIX are:

1. The ***Optim*** **Setup** program, which allows you to sign the *default* exit as part of the installation process, as described earlier in this appendix. (If you want to sign a *user-supplied* exit, you must manually run a script file after installation is completed.)
2. The **opmdsign** script file, located in the rt/sbin directory. You can run this script at any time following installation to switch to the ***Optim*** default exit. (The letter "**d**" in the script's name indicates that it is used to sign the *default* exit.)
3. The **pr0sign** program.

The two ways to sign a *user-supplied* exit in UNIX are:

1. The **opmusign** script file, located in the rt/sbin directory. You can run this script at any time following installation to switch to a user-supplied exit. (The letter "**u**" in the script's name indicates that it is used to sign a *user-specified* exit.)
2. The **pr0sign** program.

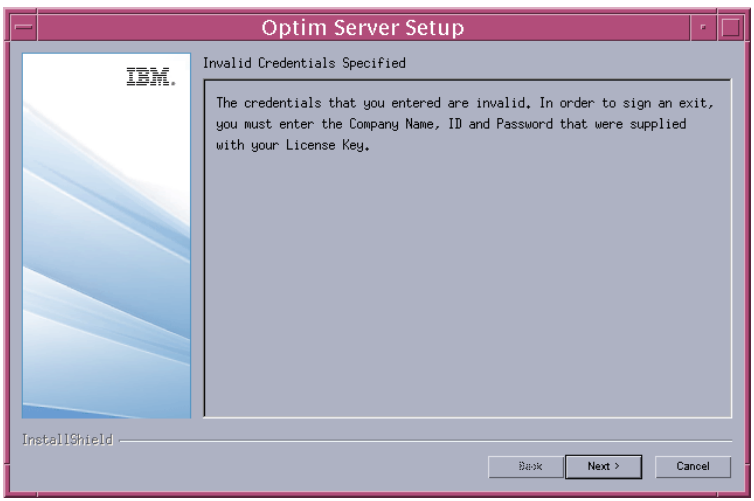
As indicated above, you can use the **pr0sign** program to sign either the default exit or a user-supplied exit. Before you run the **pr0sign** program, however, you must ensure that the environment is set up. The **opmdsign** and **opmusign** scripts will both set up the environment and call **pr0sign**.

You must sign an exit for *each* installation of ***Optim*** on a UNIX server. If you copy a signed exit from one installation to another, you must sign the exit again at the target installation.

A.5.4 The Invalid Credentials Specified Dialog

After you sign an exit, if any of the company credentials you specified are incorrect, an **Invalid Credentials Specified** dialog will appear. This usually happens if you typed your company credentials in the wrong case (i.e., uppercase verses lowercase, or vice versa), or you typed your company **Name** in a format other than the one specified for your company.

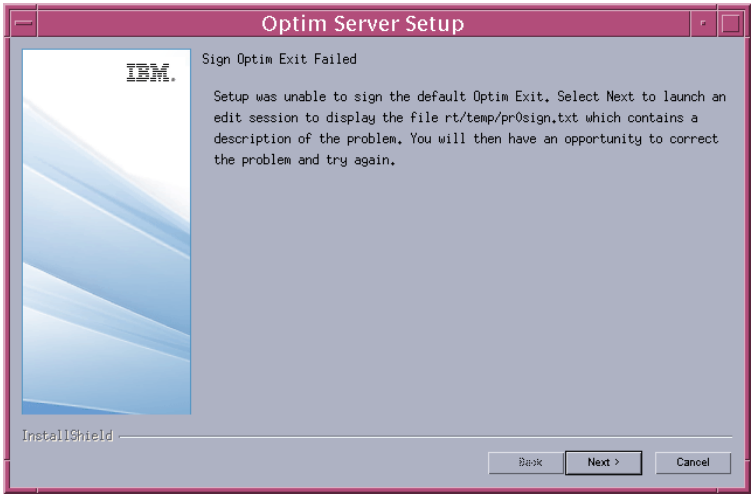
For example, if the "company name" assigned to your organization consists of all lowercase letters (such as "abc company"), you must type your company's name in all lowercase letters; otherwise, the **Invalid Credentials Specified** dialog will appear.


Optim Server Setup
IBM.
Invalid Credentials Specified
The credentials that you entered are invalid. In order to sign an exit, you must enter the Company Name, ID and Password that were supplied with your License Key.
InstallShield
Back
Next >
Cancel

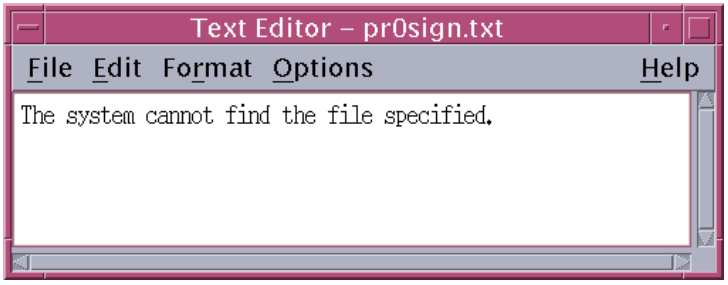
If the **Invalid Credentials Specified** dialog appears, click **Next** to redisplay the **Sign Optim Exit** dialog. Then repeat the signing process by typing your company credential in the proper format. If needed, refer to the company credential you received along with ***Optim*** to determine the proper format for this information.

A.5.5 The Sign Optim Exit Failed Dialog

As noted above, the **Invalid Credentials Specified** dialog displays errors pertaining to the *company credentials* specified during the signing of an exit. The **Sign Optim Exit Failed** dialog will notify you about any other exit-related errors. For example, if the ***Optim*** module used to challenge an exit's signing is corrupted or missing, the **Sign Optim Exit Failed** dialog will appear.


Optim Server Setup
IBM.
Sign Optim Exit Failed
Setup was unable to sign the default Optim Exit. Select Next to launch an edit session to display the file rt/temp/pr0sign.txt which contains a description of the problem. You will then have an opportunity to correct the problem and try again.
InstallShield
Back
Next >
Cancel

It is important to understand that this dialog only *notifies* you that there was an unspecified error in the signing process. Detailed information about the actual error will appear in a separate, text editor window after you click **Next**. ***Optim*** will extract the appropriate error information from a **pr0sign.txt** file, as shown in the following example.



In the above example, the signing process failed because the module used to challenge the signing is missing. (The information displayed in

the text editor is stored for future reference in the **pr0sign.txt** file in the **rt/temp** directory.)

Optim will display the **Sign Optim Exit** dialog, along with the text editor window, so you can do one of the following:

- If you can resolve error, you can sign the exit.
- If you cannot resolve the error, select **No** in response to the question "Do you want to sign the default Optim Exit," and then click **Next**. After ***Optim*** is installed, you can fix the problem that caused the error, and then sign the exit you want to use by running either:
  - the **opmdsign** script file to sign the default exit, or
  - the **opmusign** script to sign a user-supplied exit of your own creation.

A.5.6 Signing the Default Exit after an Installation

After ***Optim*** is installed, there are two options available in UNIX to sign the default exit (if you did not sign that exit during setup):

- Run the script file **opmdsign**, located in the rt/sbin directory. (The letter '**d**' in the script's name indicates that it is used to sign the *default* exit.)
- Run **Setup** again, but do not select any components for installation.

Run the opmdsign Script

As part of setup, ***Optim*** places the script file **opmdsign** in the **rt/sbin** directory. When you use **Setup** to sign the default exit, it launches this script file to set up the environment and calls **pr0sign**.

You may also run the **opmdsign** script file at any time following setup to sign the default exit. Before you do that, however, make sure that no ***Optim*** processes are running.

The syntax for **opmdsign** is as follows:

opmdsign *install_directory/**rt*** *[Company Id]* *[Name* *[Password]*]

Parameter	Identifies
install_directory/rt	the **rt** subdirectory appended to your install directory

Company Id	the six-digit Id assigned to your company
Name	the Name assigned to your company
Password	the Password assigned to your company

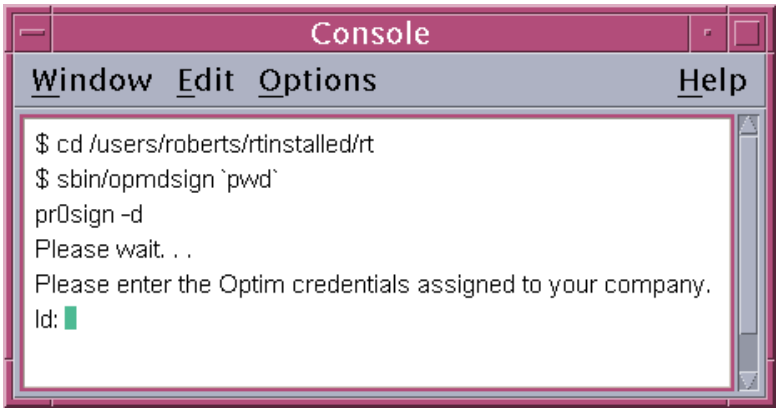
- These parameters are positional, so you must enter them in the order shown above.
- The install directory parameter (install_directory/rt) is required; the remaining parameters (Id, Name, and Password) are optional.
- If you specify a Name, you also must specify the company's Id.
- If the company's Name contains spaces, type the name in double quotes, such as "Sample Company".
- If you specify a Password, you also must specify the company's Id and Name.

The following examples show three different ways of using the **opmdsign** script to sign the default exit, following ***Optim*** installation. In all three examples, the path for the ***Optim*** installation directory is **/users/roberts/rtinstalled**.

opmdsign Signing Example # 1

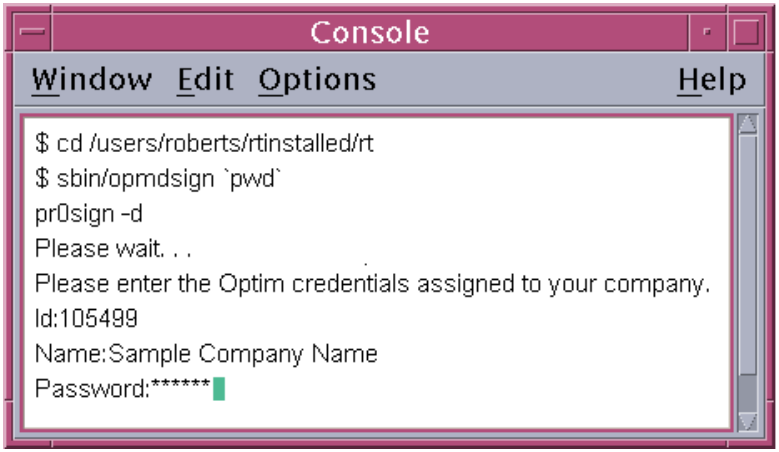
Do the following to sign the default exit after installation:

1. Shut down the ***Optim*** server if it is running.
2. Change to the **/users/roberts/rtinstalled/rt** directory. Notice the "**rt**" subdirectory appended to the install directory; this is required.
3. Run the **opmdsign** script in the **rt/sbin** subdirectory and specify the present working directory. In the following example, the user specified the system variable **`pwd`** to indicate that **/users/roberts/rtinstalled/rt** is the present working directory. (The **`pwd`** variable has the same effect as specifying the directory's full path.)



Note: In the above example, the "**pr0sign -d**" parameter shown on the third line was generated by the signing script to indicate the *default* script is being signed.

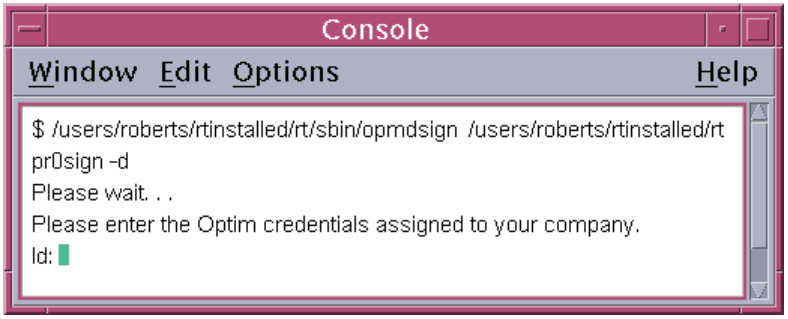
4. Type your company credentials when prompted for that information. Your company credentials consist of the company **Id**, **Name**, and **Password** assigned to your organization when you received ***Optim***. All three entries are case sensitive, and you must enter them in the format provided to you. Press **Enter** after each prompt to display the next prompt. After you specify your company **Id**, for example, press **Enter** to display the **Name** prompt.



Note: The **Name** assigned to your company may not match the spelling or punctuation used in your company's actual name.

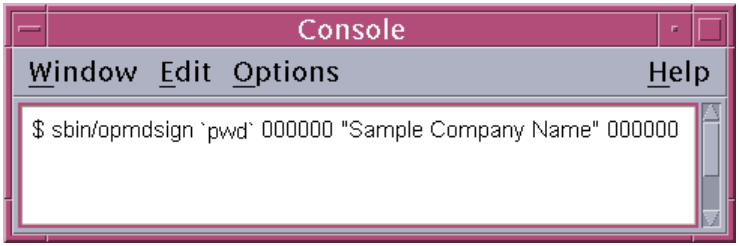
opmdsign Signing Example # 2

As in Example # 1, shut down the ***Optim Server*** if it is running, and then specify the directories explicitly, as indicated on the first line of the following example.


Console
Window Edit Options Help
$ /users/roberts/rtinstalled/rt/sbin/opmdsign /users/roberts/rtinstalled/rt pr0sign -d
Please wait. . .
Please enter the Optim credentials assigned to your company.
Id:

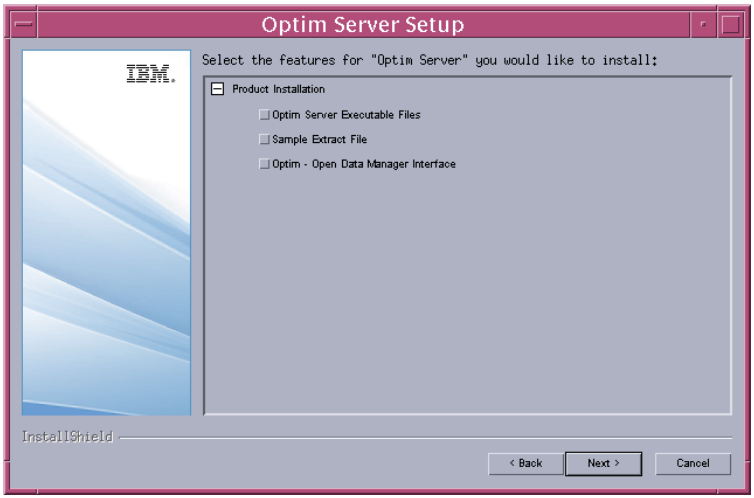
opmdsign Signing Example # 3

Do steps 1 and 2 in Example # 1 (i.e., shut down the ***Optim Server*** if it is running and then change to the **/users/roberts/rtinstalled/rt** directory). Then run the **opmdsign** script in the **rt/sbin** subdirectory, but specify all of the parameters explicitly, enclosing the company name in double quotes, as shown below.



Run Setup Again

If you have the installation CD or image available, run **Setup** again. When the following dialog appears, clear the check boxes for all listed components, as indicated below, to skip the install step and proceed to the **Sign Optim Exit** dialog.



A.5.7 Signing a User-Supplied Exit in UNIX

If your company requires the additional functionality available via a user-supplied exit, you can create your own exit, and then sign that exit as your ***Optim*** exit. (See the **Optim Initialization Exit Programmer's Guide** for detailed information on how to write an exit.)

User-Supplied Exit Prerequisites

Before you can sign a user-supplied exit, you must do the following:

1. Compile your user-supplied exit and create a load library named **libopmexit.so** (in AIX, Solaris, and Linux) or **liboptmexit.sl** (in HPUX).
2. Make sure the ***Optim Server*** is not running; if it is, shut it down.
3. Copy the file **libopmexit.so** or **libopmexit.sl** to the **rt/bin** directory, thereby overwriting the existing file, assuming one already exits.

Run the opmusign Script

As part of setup, ***Optim*** places the script file **opmusign** in the **rt/sbin** directory. You can run the **opmusign** script at any time following setup to sign a user-supplied exit. (The letter "**u**" in the script's name indicates it is used to sign a *user-specified* exit.)

The syntax for **opmusign** is as follows:

opmusign *install_directory/**rt*** *[Company Id]* *[Name* *[Password]]*

Parameter	Identifies

install_directory/rt	the **rt** subdirectory appended to your install directory
Company Id	the six-digit Id assigned to your company
Name	the Name assigned to your company
Password	the Password assigned to your company

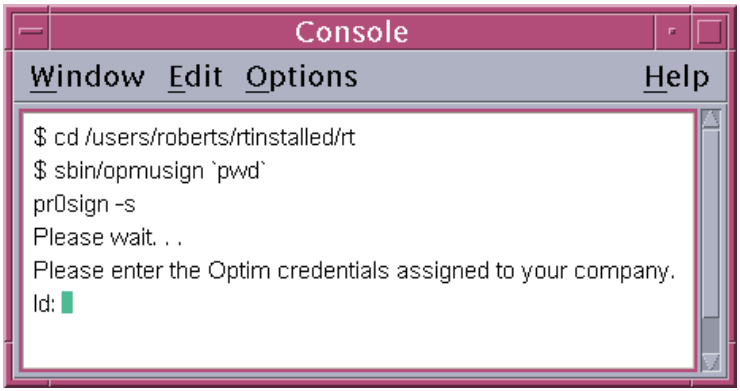
- These parameters are positional, so you must enter them in the order shown above.
- The install directory parameter (install_directory/rt) is required; the remaining parameters (Id, Name, and Password) are optional.
- If you specify a Name, you also must specify the company's Id.
- If the company's Name contains spaces, type the name in double quotes, such as "Sample Company".
- If you specify a Password, you also must specify the company's Id and Name.

The following examples show three different ways of using the **opmusign** script to sign a user-supplied exit, following ***Optim*** installation. In all three examples, the path for the ***Optim*** installation directory is **/users/roberts/rtinstalled**.

opmusign Signing Example # 1

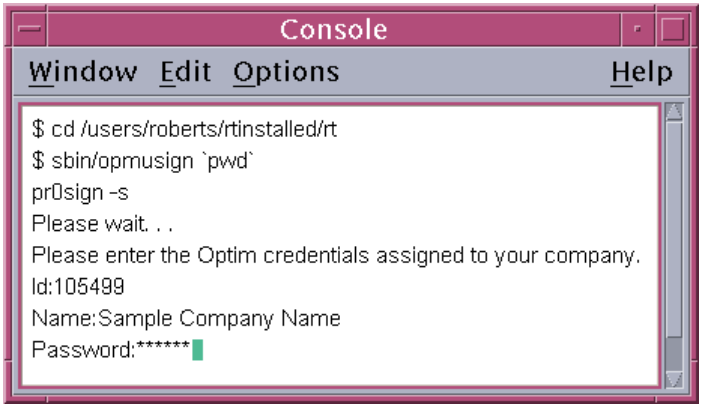
Do the following to sign your user-supplied exit after installation:

1. Shut down the ***Optim Server*** if it is running.
2. Change to the **/users/roberts/rtinstalled/rt** directory. Notice the "**rt**" subdirectory appended to the install directory; this is required.
3. Run the **opmusign** script in the **rt/sbin** subdirectory and specify the present working directory. In the following example, the user specified the system variable **`pwd`** to indicate that **/users/roberts/rtinstalled/rt** is the present working directory. (The **`pwd`** variable has the same effect as specifying the directory's full path.)



Note: In the above example, the "**pr0sign -s**" parameter shown on the third line was generated by the signing script to indicate a *user-supplied* script is being signed.

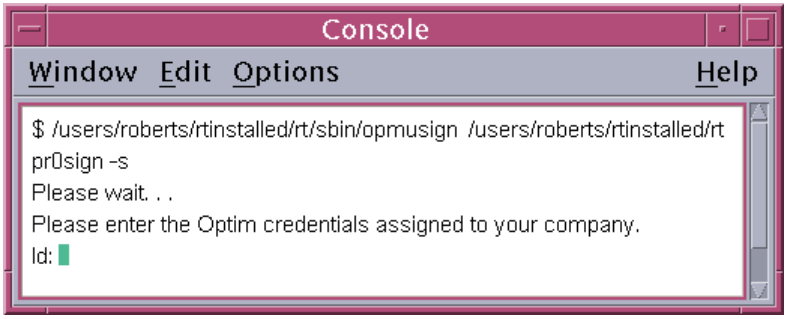
4. Type your company credentials when prompted for that information. Your company credentials consist of the company **Id**, **Name**, and **Password** assigned to your organization when you received ***Optim***. All three entries are case sensitive, and you must enter them in the format provided to you. Press **Enter** after each prompt to display the next prompt. After you specify your company **Id**, for example, press **Enter** to display the **Name** prompt.



Note: The **Name** assigned to your company may not match the spelling or punctuation used in your company's actual name.

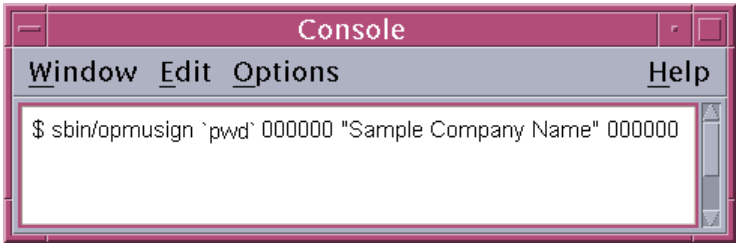
opmusign Signing Example # 2

As in Example # 1, shut down the ***Optim Server*** if it is running, and then specify the directories explicitly, as indicated on the first line of the following example.



opmusign Signing Example # 3

Do steps 1 and 2 in Example # 1 (i.e., shut down the ***Optim Server*** if it is running and then change to the **/users/roberts/rtinstalled/rt** directory). Then run the **opmusign** script in the **rt/sbin** subdirectory, but specify all of the parameters explicitly, enclosing the company name in double quotes, as shown below.



Appendix B. Server Credentials

This appendix provides information about credentials used with the ***Optim Server*** (***Server***) feature of ***Optim***. The ***Server*** can be installed and run on a machine using supported versions of Windows, Solaris, HP-UX, AIX, or Linux; therefore, this appendix addresses credentials for all supported platforms.

Credentials uniquely identify a user, and include:

- User ID
- Password
- Domain (for Windows only)

The following types of credentials are used with the ***Server***:

- Credentials needed to run the ***Server*** and to start ***Optim*** processes.
- Credentials needed by the DBMS to access the ***Optim*** Directory and use the DB Alias.

B.1 *Server* Credentials

Credentials required by the ***Server*** include a User ID, Password, and Domain (for Windows only). You must provide ***Server*** credentials for the following users.

- The user account under which the ***Server*** runs.
- The user account under which ***Optim*** processes run.

At installation, the default is to run the ***Server*** under the Local System Account and ***Optim*** processes under the credentials from the initiating workstation. The Local System Account is a special account for Services only that has full access to the local machine. However, the Local System Account cannot access mapped network drives.

You can provide other ***Server*** credentials on the **Startup** tab and the **Security** tab of the **Optim Server Settings** applet, and the **Server** tab of Personal Options. For UNIX or Linux, you can specify ***Server*** credentials using the **filelogon** parameter of the pstserv configuration file (pstserv.cfg) and the **server** parameter of the pstlocal configuration file (pstlocal.cfg).

Note: For information about the **Optim Server Settings** applet, see **Chapter 6. Configure the Optim Server**; for details about Personal Options, see **9.2.9 Server Tab** on page 305; and for information about UNIX and Linux configuration files, see **A.2 Configuration** on page 358.

B.1.1 Credentials to Run the *Server*

Credentials to run the ***Server*** are determined by the following:

Windows	The **Startup** tab of the **Optim Server Settings** applet. If not using the Local System account, you provide the credentials in **User ID**, **Password**, and **Domain**.
UNIX or Linux	The User ID under which the ***Server*** (pr0svce) daemon is executed.

After startup, the User ID for the ***Server*** may require other privileges, depending on whether you are using explicit credentials or client credentials.

For Windows, credentials on the **Startup** tab of the **Optim Server Settings** applet are added to the Service Control Manager database. At a minimum, the user account must have the authority to log on to the local computer as a service. You can use the Local Security Policy to grant this authority or you can use the built-in Local System Account, which has full authority on the local computer.

For UNIX or Linux, the user account under which the ***Server*** daemon is started dictates the privileges for the daemon. If the daemon is started as part of INIT processing, you must log on with the proper User ID before starting the daemon, or use the SU (substitute user) command.

B.1.2 Credentials to Run *Optim* Processes

Every ***Optim*** process initiated by a client, whether online (from a Request Editor) or from the Command Line Interface or the ODBC Interface, is run in its own process under the ***Server***. This allows you to start individual processes under explicit user credentials and run multiple processes simultaneously without interfering with each other.

You can choose the credentials used to start these processes.

- Run the process under the user account that was used to start the ***Server***.
- Run the process under an explicitly designated user account, regardless of the initiating account (i.e., Request Editor, Command Line Interface, or ODBC Interface).
- Run the process under the initiating user account.

These credentials determine the network access allowed for the process, and, for Oracle OS Authentication or the Informix Loader, the User ID used for DBMS access.

The credentials are verified by the system and must include a valid User ID known to the specified security provider. For Windows, an actual logon for the specified user occurs and the process is started under those credentials, as if the user logged on from the console directly. For UNIX or Linux, the effective User ID and Group ID for the process are changed to the credentials specified for running ***Optim*** processes.

Run Under Server Credentials

You can run processes under the authentication provided by the ***Server*** credentials. This limits access to the files local to the ***Server*** machine or, at least, to the files that are accessible with the ***Server*** credentials.

Select ***Server*** credentials for processes, as follows:

Windows	On the **Security** tab of the **Optim Server Settings** applet, select **Server** for the **File Input/Output** option and select the **Only files local to this Server may be accessed** check box.
UNIX or Linux	For pstserv.cfg, set the **filelogon** parameter to "local."

Note the following when you use the ***Server*** credentials to run processes:

- For Windows, a service running under Local System Account cannot be logged on to the network. (See **B.1.4 UNC Network Share Access (Windows)** for more information.)
- Oracle OS Authentication will run under the user that started the service (Windows) or daemon (UNIX or Linux). Oracle requires a known User ID (established by an administrator); therefore, you cannot use the Local System Account for Windows. Informix Loader, which uses credentials for the currently logged on user, also requires a known User ID. (For more information, see **B.1.6 Oracle OS Authentication**.)
- For UNIX or Linux, mount points for networked shares or file access are allowed according to the effective User or Group accounts for the process. Therefore, all processes can use files available to the User account under which the ***Server*** daemon is started. (For more information, see **B.1.7 UNIX or Linux File Access**.)

Run Under Explicit Credentials

You can run processes under an explicit user account to control network access and DBMS logons that use the account for the process (for Oracle OS Authentication and Informix Loader).

You can use the ***Server*** to access ***Optim*** Directories, DB Aliases, and network shares that individual clients cannot access, and simply restrict the users that can log on to the ***Server*** machine. You must require that the credentials in the **Optim Server Settings** applet (Windows) or

pstserv.cfg (UNIX or Linux) be used instead of credentials from the initiating clients, as follows:

Windows	On the **Security** tab of the **Optim Server Settings** applet, select **Server** for the **File Input/Output** option, clear the **Only files local to this Server may be accessed** check box, and provide explicit credentials in **User ID**, **Password**, and **Domain**.
UNIX or Linux	For pstserv.cfg, set the **filelogon** parameter to "server" and provide an explicit User ID and password.

Note: The ***Server*** credentials must have specific rights, as specified in **B.1.3 Server Privileges for Explicit or Client Credentials**.

Run Under Client Credentials

You can run processes under the credentials from the workstation used to initiate the process. The process is run with the same rights as if it were run on the initiating machine as a LOCAL request.

Require the use of initiating credentials on the ***Server*** as follows:

Windows	On the **Security** tab of the **Optim Server Settings** applet, select **Client** for the **File Input/Output** option.
UNIX or Linux	For pstserv.cfg, set the **filelogon** parameter to "client."

Also, on each initiating machine, you must provide the credentials for the ***Server***.

Windows	On the **Server** tab in Personal Options, enter the credentials for all (Default) or individual ***Servers***.
UNIX or Linux	In pstlocal.cfg, specify the credentials on each **server** parameter.

Note: The ***Server*** credentials must have specific rights, as specified in **B.1.3 Server Privileges for Explicit or Client Credentials**.

B.1.3 *Server* Privileges for Explicit or Client Credentials

Whether using explicit credentials or client credentials, the ***Server*** credentials require certain privileges. For Windows, the ***Server*** credentials must allow logon as a user and the creation of a process request as that user. To establish these permissions, you must access the Local Security Policy and grant the following privileges to the user.

- Act as part of the operating system (SeTcbPrivilege)
- Increase quotas (SeIncreaseQuotaPrivilege)
- Replace a process level token (SeAssignPrimaryTokenPrivilege)
- Bypass traverse checking (SeChangeNotifyPrivilege)

Note: These privileges are automatically granted to the Local System Account.

Also, the overriding User ID (specified on the **Security** tab of the **Optim Server Settings** applet) and the client credentials must have the following privilege. (Note that, in some installations, you can give this privilege to everyone in the Local Security Policy, instead of specifying credentials for each client user.)

- Log on as a batch job (SE_BATCH_LOGON_NAME)

For UNIX or Linux, "Super-User" ***Server*** credentials are required to change the effective User ID and Group ID. During startup, if the **filelogon** parameter is set to "client" or "server," the effective User ID that started the daemon must be a "Super-User" (zero).

B.1.4 UNC Network Share Access (Windows)

Mapped drives cannot be used for file names when processes are run from the ***Server***, because the drive is mapped only when the user is logged on to the interactive desktop. Mapping is removed when the user logs off or disconnects from the share. Thus, a file that is valid when the request is created may be invalid at run time.

To specify network files, use a Universal Naming Convention (UNC), in the following format:

*servername**sharename*

Each file server must specify the User IDs and access rights (read, write, execute, and so on) for each of its shares. The User ID that is sent to

these file servers is the User ID used to run the process (i.e., using ***Server*** credentials, explicit credentials, or client credentials).

The following restrictions apply.

- The share on the file server can specify the User ID from that Domain (or everyone).
- The share on the file server can specify the ***Server*** machine name and the User ID (or everyone).
- You cannot specify Local System Account on a file server, since there is no external name associated with this credential. When a connection is made to the file server, the "guest" (or anonymous) account is used; therefore, the network share must specify that the guest account (or everyone) has access to the share.

B.1.5 Registry Access for Process Requests (Windows)

The ***Server*** component always uses the Local Machine hive in the registry, which is always available.

The user credentials used to start the process can be the Local System Account, a local user, or a domain user. Only local users (or domain users that have previously logged on to the ***Server*** machine) have a current user hive; others use the default user hive, HKEY_USERS\.DEFAULT, instead.

When using the default user hive, any changes are only cached in memory for use by the process, and are not recorded to the registry. Also, you cannot make the default user hive your current user hive if you log on to the interactive desktop for the ***Server***.

While this is not a problem for the ***Server*** processes, this may be problematic for registry settings needed by the DBMS. For example, Informix requires certain registry settings that are recorded in the current user hive for the user logged on at the time that the Informix utilities are used (SETNET32). To correct this issue, once you set up the options, you can copy them to the default user hive using the REGCOPY utility. You must re-run the REGCOPY utility each time you change the options.

B.1.6 Oracle OS Authentication

If you set up Oracle to allow OS Authentication (which is beyond the scope of this document), ***Optim*** must use the current User ID for the process to be used by Oracle. Enter one forward slash (/) for the User ID and leave the Password blank.

B.1.7 UNIX or Linux File Access

The effective User ID and Group ID for a process determine the directories, files, or mount points that can be accessed. By default, the user that creates a file has read and write privileges; any other group or user has read privileges only.

Filemode Parameter

You may want files created by the ***Server*** to be available to other users to run the same job and overlay the same file. The **filemode** parameter in pstserv.cfg allows you to grant file access to other users. The **filemode** parameter changes the default file mode for any file created by the ***Server*** and allows you to limit read or write privileges for a user, group, or other.

Daemon Startup Directory

A directory created during the daemon startup tracks the daemon system-wide, so that you can shut the daemon down from a different process. This directory includes a file for each daemon started. (In production environments, there is usually one file.)

The default creates an “rt4s” subdirectory under the system “tmp” directory. However, the daemon is often run under a “fenced” user that does not have privileges in the tmp directory. To overcome this, you can set the PSTINFO environment variable before starting the daemon. Specify the complete path to a directory to which the user starting the daemon can write. In general, you must pre-create the directory to give it specific user rights.

B.2 DBMS Logon Credentials

DBMS logon credentials needed to access the ***Optim*** Directory and use the DB Alias include a User ID, Password, and Connection String. If using the ***Server***, you can provide the DBMS logon credentials in two places:

- The **Connections** tab of the **Optim Server Settings** applet.
- The **Logon** tab of Personal Options.

The location used to maintain DBMS logon credentials depends on the settings on the **Security** tab of the **Optim Server Settings** applet, or the **pstlogon** or **dbaliaslogon** parameters in the pstserv configuration file (pstserv.cfg) for UNIX or Linux.

Optim Directory Access

To use the ***Optim*** Directory information from the ***Server***:

Windows	On the **Security** tab of the **Optim Server Settings** applet, select **Server** for the **Optim Directories** option.
UNIX or Linux	For pstserv.cfg, set the **pstlogon** parameter to "server."

To use the ***Optim*** Directory information from each initiating client:

Windows	On the **Security** tab of the **Optim Server Settings** applet, select **Client** for the **Optim Directories** option.
UNIX or Linux	For pstserv.cfg, set the **pstlogon** parameter to "client."

DB Alias Access

To use the DB Alias information from the ***Server***:

Windows	On the **Security** tab of the **Optim Server Settings** applet, select **Server** for the **DB Aliases** option.
UNIX or Linux	For pstserv.cfg, set the **dbaliaslogon** parameter to "server."

To use the DB Alias information from each initiating client:

Windows	On the **Security** tab of the **Optim Server Settings** applet, select **Client** for the **DB Aliases** option.
UNIX or Linux	For pstserv.cfg, set the **dbaliaslogon** parameter to "client."

Maintain DBMS Logon Credentials

The connection string you specify on the **Optim Server Settings** applet (for Windows) or in the configuration file (for UNIX or Linux) is always used, regardless of whether Server or Client is the source of the credentials for ***Optim*** Directory and DB Alias access. You must specify a connection string to access an ***Optim*** Directory and use a DB Alias; otherwise, the ***Optim*** process will fail.

If Server is the source of DBMS logon credentials, specify the following:

Windows	On the **Connection** tab of the **Optim Server Settings** applet, provide a **User ID**, **Password**, and **Connection String**.
UNIX or Linux	For pstlocal.cfg, provide a *userid*, *password*, and *connect-string* for the **pstdir** and **dbalias** parameters.

If Client is the source of DBMS logon credentials, specify the following for the ***Server*** machine:

Windows	On the **Connection** tab of the **Optim Server Settings** applet, provide a **Connection String** only (**User ID** and **Password** are ignored).
UNIX or Linux	For pstserv.cfg, provide a *connect-string* for the **pstdir** and **dbalias** parameters (*userid* and *password* are ignored).

Also, if Client is the source of DBMS logon credentials, you must specify the following for the client machine:

Windows	On the **Logon** tab in Personal Options, provide the **User ID** and **Password**. Also, provide a valid **Connection String** for the client to connect to the ***Optim*** Directory and use the DB Alias.

UNIX or Linux For pstlocal.cfg, provide a *userid* and *password* for the **pstdir** and **dbalias** parameters. Also, provide a valid *connect-string* for the client to connect to the ***Optim*** Directory and use the DB Alias.

Appendix C. Command Line Maintenance Tasks

Optim provides a Command Line Interface that allows you to perform certain configuration tasks, without using the graphical user interface for ***Optim***. You can run the Command Line Interface from the command line, in a batch file, or from another program.

Command Line Tasks

You can use the Command Line Interface to:

- Create one or more DB Aliases.
- Update (refreshing the DB signature) one or more DB Aliases.
- Apply maintenance to one or more DB Aliases.
- Apply maintenance to one or more ***Optim*** Directories.

The following sections explain and describe how to perform each of these tasks.

Guidelines

The typical command consists of PR0CNFG followed by keywords and associated arguments. The following guidelines apply:

- All keywords must be prefixed by a forward slash (/) or a dash (-) and separated from one another by one or more spaces. Do not use commas.
- Keywords must be separated from arguments by an equal sign (=) or a colon (:).
- Using a keyword that is inappropriate for the type of processing may cause a fatal conflicting-parameter error.
- The DBMS type keyword must precede the DBMS version keyword. All other keywords can be specified in any order.

- If you use a keyword more than once for a task, the last instance applies.
- You can include all keywords and arguments for one or more tasks in a text file, and reference this parameter file on the command line.
- In a parameter file, keywords and arguments for a task may be on more than one line. Note that lines after the line containing the TASK keyword are processed in the next task, if any.
- If a keyword required for a task is omitted, values specified for the previous task, or values specified the last time the **Configuration** program was run, are used by default.

  Note: This feature may be advantageous for a series of tasks that share the same setting for one or more parameters.
- An argument that includes spaces must be enclosed in single or double quotes.
- To clear a parameter, specify the value as an empty string, i.e., “ ” .

Syntax Conventions

The syntax conventions used to describe these statements are:

KEYWORD	Keywords are shown in uppercase for emphasis, but can be specified in lower or mixed case.
text	Variable text is shown in lowercase italics.
( )	Statement delimiter to group a series of qualifiers for a parameter.
[ ]	An optional keyword or argument is shown in square brackets.
{ }	A choice of settings from which only one must be selected is shown in curved brackets.
< >	A choice of settings from which none or any may be selected is shown in angle brackets.
|	Separates options.

C.1 Syntax and Keywords

Use the following command line syntax:

General

PR0CNFG [/NOLOGO] /FILE={ *filename* |
/AUTORUN={ TRUE | FALSE | ON | OFF | YES | NO }
[/RESPONDFILE=*filename*]
[/IGNORE]

***Optim* Directory**

/PSTDIRNAME={ *pstdirname* | ***currentdir*** }
/PSTDIRID=*pstdirid*
/PSTDIRCONNECTSTR=*dbmscnctionstr*
/PSTDIRPASSWORD=*password*
/PSTDIRUSERID=*userid*

DB Alias

/DBAACTION={CreateNew | UseExisting }
/DBANAME=*dbaliasname*
/CONNECTSTR=*dbmscnctionstr*
/PASSWORD=*password*
/PASSWORDREQUIRED={TRUE | FALSE | ON | OFF | YES | NO }
/USERID=*userid*
/DBMSTYPE={DB2MVS | INFORMIX | ORACLE | SYBASE |
UDB | SQLSERVER }
/DBMSVERSION=*versionnum*
/DBQUALIFIER=*databasequal*
/SPSHARE={ TRUE | FALSE | ON | OFF | YES | NO }
/DESCRIPTION="*description*"
/UNICODEDB={ TRUE | FALSE | ON | OFF }
/MULTIBYTEDB={ TRUE | FALSE | ON | OFF }

***Optim* Directory or DB Alias**

{ /SPACTION | /BINDACTION }={ CreateNew | UseExisting }
{ /SPQUALIFIER | /COLLECTIONNAME }=*name*

Task

TASK={ DB | MAINTPST | MAINTCAT } }

Keywords

General

PR0CNFG Initiate command line processing. Note that the character following PR is the number 0 (zero).

/NOLOGO Suppress the splash logo.

/FILE= The source of parameters or the parameters.

- ***filename*** The fully qualified path and name of a text file containing parameters for one or more tasks. You must enclose a ***filename*** that includes blanks in quotes.
- ***parameters*** As follows.

/AUTORUN= Level of user intervention when running.

- **TRUE, ON,** or **YES** Run the **Configuration** program in AutoRun mode, hiding dialogs unless user intervention is required to correct or cancel the task. If an error cannot be corrected, the error message is displayed on the **Log** dialog. (Default for a parameter file.)
- **FALSE, OFF,** or **NO** Run the **Configuration** program normally, displaying all dialogs. (Default for parameters from the command line.)

/RESPONDFILE= The source of default values for Message IDs when AUTORUN=ON.

- ***filename*** The fully qualified path and name of a text file. A sample file, RESPOND.PST, in the RT/BIN directory can be modified and used as necessary. You must enclose a ***filename*** that includes blanks in quotes.

/IGNORE Begin a comment or disregard parameters. All parameters that follow and are on the same line have no effect on processing.

Optim Directory

/PSTDIRNAME= ***Optim*** Directory for the task.

- ***pstdirname*** Name of the ***Optim*** Directory
- ***currentdir*** The current ***Optim*** Directory (default).

/PSTDIRID= Identifier that prefixes ***Optim*** Directory table names.

- ***pstdirid*** Schema Name, Creator ID, or Owner ID for the ***Optim*** Directory tables.

/PSTDIRCONNECTSTR= Connection to the ***Optim*** Directory.

- ***dbmscnctstr*** Name that permits access to the database containing the ***Optim*** Directory.

/PSTDIRPASSWORD= Password for connection.

- ***password*** A value is required if the Always Prompt for Password option is active for the ***Optim*** Directory.

/PSTDIRUSERID= User account with DBMS permission to connect.

- ***userid*** If **/TASK=MAINTPST**, the user account must have the authority, through System Privileges or Roles, to create the tables and to catalog the packages, plans, or procedures under the appropriate table identifier.

DB Alias

/DBAACTION= Processing indicator for the DB Alias.

- **CreateNew** Create a new DB Alias named by DBANAME.
- **UseExisting** Use the existing DB Alias indicated by DBANAME.

/DBANAME= Name of DB Alias.

- ***dbaliasname*** Required if **/TASK=DB** or **/TASK=MAINTCAT**.

/CONNECTSTR= Connection string for the database associated with the DB Alias.

- ***dbmscnctstr*** Required if **/TASK=DB** or **/TASK=MAINTCAT**.

/PASSWORD= Password for connection.

- ***password*** Required if the Always Prompt for Password option is active for the DB Alias or if creating a DB Alias using **/TASK=DB**.

/PASSWORDREQUIRED= Always Require Password option for a new DB Alias (**/TASK=DB**). Keyword is ignored for an existing DB Alias.

- **TRUE, ON,** or **YES** Always require a password.
- **FALSE, OFF,** or **NO** Save the password in the registry.

/USERID= User account with DBMS permission to connect to database associated with the DB Alias. Required if the Always Prompt for Password option is active for the DB Alias or if creating a DB Alias using **/TASK=DB**.

userid If **/TASK=DB** and you are creating a new DB Alias or if **/TASK=MAINTCAT**, the user account must have the authority, through System Privileges or Roles, to create the tables and to catalog the packages, plans, or procedures under the appropriate table identifier.

/DBMSTYPE= The DBMS associated with the DB Alias. Required if **/TASK=DB**.

DB2MVS **SYBASE**

INFORMIX **UDB**

ORACLE **SQLSERVER**

/DBMSVERSION= The version of the DBMS associated with the DB Alias. **/DBMSVERSION** must follow **/DBMSTYPE**.

versionnum Required if **/TASK=DB**.

/DBQUALIFIER= Database name.

databasequal Required if **/TASK=DB** and DBMS is Sybase ASE, SQL Server, or Informix.

/SPSHARE= Indicator for sharing Stored Procedures for multiple Sybase ASE or SQL Server DB Aliases when **/TASK=DB**.

TRUE, ON, or **YES** Stored Procedures are shared.

Notes:

For **Sybase**, stored procedures are stored in the special Sybase ASE database sybsysprocs.

For **SQL Server**, stored procedures are stored in the MASTER database. Microsoft SQL Server documentation contains a cautionary statement about creating stored procedures in the MASTER database. Consider the implications of sharing stored procedures for SQL Server before proceeding.

FALSE, OFF, or **NO** Stored Procedures are not shared.

/DESCRIPTION= Optional description for DB Alias. (**/TASK=DB**)

"description" 1 to 40 characters, delimited by double quotation marks.

/UNICODEDB= Store ***Optim*** Directory data in Unicode format.

TRUE or **ON** Store data in Unicode format.

FALSE or **OFF** Do not store data in Unicode format.

/MULTIBYTEDB= Use multibyte encoding for the DB Alias.

TRUE or **ON** Use multibyte encoding.

	FALSE or **OFF**	Do not use multibyte encoding.

Optim Directory or DB Alias

The following keywords are interchangeable, and are not DBMS dependent.

{ /SPACTION | /BINDACTION }=	Indicator for ***Optim*** Stored Procedures or ***Optim*** Bind Files.	
	CreateNew	Create new Stored Procedures or Bind Files.
	UseExisting	Use previously loaded Stored Procedures or Bind Files.
{ /SPQUALIFIER | /COLLECTIONNAME }=	***name***	Schema Name or Owner ID of the Stored Procedures, or Plan Name of the Bind Files.

Task

The TASK keyword identifies the task to be performed. If a task is entered on the command line, you must provide the parameters on the same line. When using a parameter file, the TASK keyword signals the end of a list of parameters for a task; keywords on lines following a TASK keyword are processed in the next task, if any, or are ignored if no new TASK keyword is found.

TASK=	The task identifier, as follows:	
	DB	Create or update a single DB Alias.
	MAINTPST	Apply maintenance to a single ***Optim*** Directory.
	MAINTCAT	Apply maintenance to a single DB Alias.

C.2 Examples

C.2.1 Create Multiple DB Aliases with one Optim Directory

The first step is to create a text file with the appropriate parameters for the tasks. For this example, the text file is called C:\Cre_dba.txt:

```
/PSTDirName=ORA_LOCAL    /PSTDirUserID=roberts
    /PSTDirPassword=softech      /DBAAction=createnew
    /DBAName=AUDB_LOCAL  /DBMSType=UDB
    /DBMSVERSION=6.1
    /ConnectStr=sample  /UserID=roberts   /Password=robbie
    /SPAction=createnew  /Description="Local UDB V 6.1 Sample"
    /Task=DB

/DBAAction=createnew   /DBAName=ASYB_LOCAL
    /DBMSType=SYBASE   /DBMSVERSION=11.9.2
    /ConnectStr=roberts    /UserID=roberts   /Password=robbie
    /DBQualifier=roberts   /SPAction=createnew    /SPShare=True
    /Description="Local Sybase V 11.9.2 roberts"  /Task=DB

/DBAAction=createnew  /DBAName=AROBDB3
    /DBMSType=SYBASE   /DBMSVersion=11.9.2
    /ConnectStr=roberts
    /UserID=roberts  /Password=robbie  /DBQualifier=robdb3
    /SPAction=Useexisting   /SPShare=True   /Description="Local
    Sybase V 11.9.2 robdb3"  /Task=DB

/DBAAction=createnew  /DBAName=AROBDB4
    /DBMSType=SYBASE   /DBMSVersion=11.9.2
    /ConnectStr=roberts
    /UserID=roberts  /Password=robbie  /DBQualifier=robdb4
    /SPAction=UseExisting  /SPShare=True   /Description="Local
    Sybase V 11.9.2 robdb4"  /Task=DB
```

To perform the tasks from the command line, specify:

PR0CNFG /FILE=C:\Cre_dba.txt

C.2.2 Apply Maintenance to Multiple DB Aliases

The first step is to create a text file with the appropriate parameters for the tasks. For this example, the text file is called C:\Maint_dba.txt:

```
/PSTDirName=ORA_LOCAL    /PSTDirUserID=roberts
     /PSTDirPassword=softech   /DBAAction=useexisting
     /DBAName=AUDB_LOCAL    /UserID=roberts
     /PASSWORD=fido      /Task=MAINTCAT

/DBAAction=useexisting  /DBAName=ASYB_LOCAL
      /Task=MAINTCAT

/DBAAction=useexisting  /DBAName=AROBDB3
      /Task=MAINTCAT

/DBAAction=useexisting  /DBAName=AROBDB4
      /Task=MAINTCAT

/DBAAction=useexisting  /DBAName=AORA_LOCAL
      /Task=MAINTCAT

/DBAAction=useexisting  /DBAName=AMSSQL_LOCAL
      /Task=MAINTCAT

/DBAAction=useexisting  /DBAName=AIFX_LOCAL
      /Task=MAINTCAT

/DBAAction=useexisting  /DBAName=AIFX_LOCALNA
      /Task=MAINTCAT

/DBAAction=useexisting  /DBAName=APSTDSNY
       /Task=MAINTCAT
```

To perform the tasks from the command line, specify:

PR0CNFG /FILE=C:\Maint_dba.txt

Appendix D. *Optim* Security

Optim provides three types of security. For each ***Optim*** Directory, you may establish any or all of the following types of security: Functional Security, Object Security, and Archive File Security.

Functional Security

As the most general level of ***Optim*** Security, Functional Security allows you to control user access to the interface for functions provided by ***Optim***. For example, for a specialized administrator role that is intended to create process requests and objects needed to run these requests, you can grant unlimited access to functions. For members of a role intended only to run the pre-defined process requests, however, you can grant more limited access to functions. As a second example, you might use Functional Security to grant access to the ***Archive***-specific editors (Archive Request, Delete Request, and Restore Request) as well as the ***Archive*** maintenance utilities to members of a specialized Archive role while denying access to these editors for developers that use ***Optim*** functions to create test data.

Establishing Functional Security requires that you edit the Access Control Domain (ACD) named **(Default)** to define roles and, for each role, grant or deny Functional Privileges. The **(Default)** ACD is a security definition (i.e., a type of object in the ***Optim*** Directory) and is created automatically when ***Optim*** Security is initialized. Functional Privileges are defined in the **(Default)** ACD only. After editing the **(Default)** ACD, you must enable Functional Security using the **Configuration** program for the Functional Security settings to take effect.

You can also use Functional Security to define Object Association Privileges, which determine the ACDs a role can associate with Access Control Lists (ACL), used by Object Security to secure objects. Within each ACD, you can define Object Association Privileges for specific object types. For example, if an ACD denies a role the Associate Archive Requests privilege, the role cannot use that ACD in an ACL that secures an Archive Request.

To establish Functional Security:

1. Using the **Configuration** program, initialize ***Optim*** Security and assign a Security Administrator as described in **5.1.4 Optim Security** on page 128.
2. Edit the **(Default)** ACD to map roles to network accounts.
3. For each role, grant or deny the appropriate Functional Privileges, and if Object Security will also be enabled, grant or deny the appropriate Object Association Privileges, as described in **Assigning Privileges** on page 457.
4. Using the **Configuration** program, enable Functional Security, as described in **7.4.3 Set Functional Security Option** on page 196.

Object Security

Object Security allows you to control access to specific objects in the ***Optim*** Directory, using an Access Control List (ACL). Any ***Optim*** object can be secured by associating it with an ACL. An ACL lists roles and grants or denies privileges for each role to read, update, delete, or execute (where appropriate) the object and the ACL. For example, you might define an ACL to allow members of a role to read and execute, but not edit, a specific Archive Request. ***Optim*** can also be configured to secure objects automatically so that a default ACL (which can be edited) is defined when the object is saved to the ***Optim*** Directory.

Note: When Object Security is enabled, the size of the fully-qualified name for a Primary Key and a Relationship is restricted, as described in the **Common Elements Manual**, **Object Security and Object Names**.

The roles in an ACL are defined in an ACD associated with the ACL. If Functional Security is enabled, a member of a role that is granted an Object Association Privilege in an ACD for an object type (e.g., Associate Access Definition privilege) can use the ACD to define roles in an ACL for that object type. Object Association Privileges are not required to use Object Security; however, these privileges must be defined to secure objects if both Functional and Object Security are enabled.

Once an object is associated with an ACL it is considered to be "secured," although Object Security must be enabled for the security defined in the ACL to be effective. ACDs and File Access Definitions

are automatically associated with an ACL, whether or not Object Security is enabled using the **Configuration** program.

To establish Object Security:

1. Using the **Configuration** program, initialize ***Optim*** Security and assign a Security Administrator as described in **5.1.4 Optim Security** on page 128.
2. Using the **Configuration** program, enable Object Security, as described in **7.4.4 Set Optim Object Security Option** on page 197:
   - Indicating whether selected objects are automatically assigned an ACL when saved.
   - Defining the Object Template ACL.
3. Edit the **(Default)** ACD and any additional ACDs to map roles to network accounts.

Archive File Security

Archive File Security allows you to control access to data in Archive Files. For example, you might use Archive File Security to prevent any access to data in a specific table or column for most users while granting access to members of selected roles for the same data. Each secured Archive File is associated with a File Access Definition (FAD), which is a security definition that lists tables and columns for which access privileges are defined and, for each listed role, grants or denies privileges to access the archived data.

Establishing Archive File Security requires an ACD (the **(Default)** ACD or one you create for the purpose) used as the basis for roles in the FAD. In addition, you must use the **Configuration** program to enable Archive File Security.

To establish Archive File Security:

1. Using the **Configuration** program, initialize PST Security and assign a Security Administrator as described in **5.1.4 Optim Security** on page 128.
2. Using the **Configuration** program, enable Archive File Security, as described in **7.4.5 Set Archive File Security Option** on page 200.
3. Edit the **(Default)** ACD and any additional ACDs to map roles to network accounts.

4. Create and edit each FAD, using roles in the appropriate ACD.
5. Reference the appropriate FAD in each Archive Request used to create secured Archive Files.

Access Control Domains

The Access Control Domain is a security definition that serves as the foundation for all levels of ***Optim*** Security. Each ***Optim*** Directory for which ***Optim*** Security is initialized contains an ACD named **(Default)** that cannot be deleted. Depending upon the needs of your facility, you may create additional ACDs or use only the **(Default)** ACD. Each ACD includes a list of roles. Each role represents a logical grouping of user and group accounts in your network. Typically you might assign names of roles to convey the capabilities of the accounts represented by the role. Examples of role names might be "GUEST", "NORMAL", and "SUPER". User and group accounts are mapped to one or more roles, as appropriate.

The role specifications in the **(Default)** ACD are referenced for Functional Security, if enabled for the ***Optim*** Directory. Also, the role specifications in the **(Default)** or other ACD are referenced by Access Control Lists (used to secure objects) and File Access Definitions (used to secure Archive Files) and assigned privileges to access the object or Archive File.

Access Control List

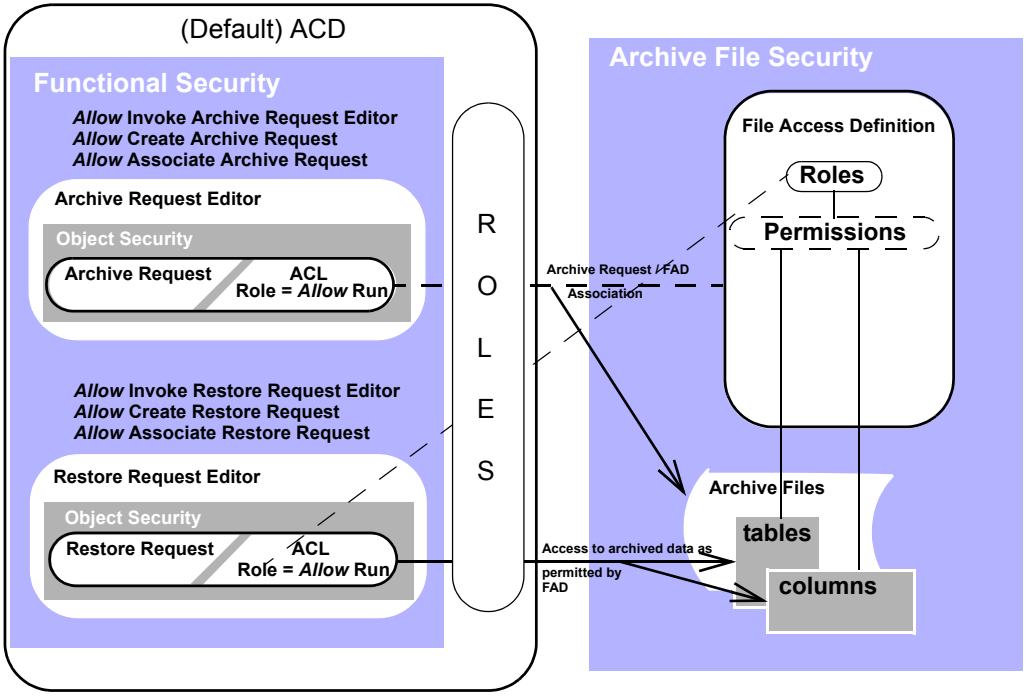
The Access Control List is an ***Optim*** object that serves as the basis for Object Security. ACL parameters govern the ability of a role to perform actions (such as read, update, or delete) on both the object and the ACL for the object. Each ACD, File Access Definition, and secured ***Optim*** object has a unique ACL.

File Access Definition

The File Access Definition is the basis for Archive File Security. All Archive Files generated by running an Archive Request that references an FAD are secured by the FAD.

Security Diagram

The following diagram illustrates the features of ***Optim*** Security.



The **(Default)** ACD, an object in the ***Optim*** Directory, is the linchpin for the three levels of ***Optim*** Security. In the **(Default)** ACD, arbitrarily named roles are linked to network accounts used as logons when performing tasks.

Functional Security

The **(Default)** ACD selectively grants and denies Functional Security privileges for roles in order to provide appropriate access to the interface and functions. For example, a member of a role expected to run an Archive Request online must be allowed the Invoke Archive Request Editor privilege, while a member of a role expected to create a secured Archive Request must be allowed the Create Archive Request and Associate Archive Request privileges.

Object Security

Secured objects (including ACDs and File Access Definitions) have an ACL that grants and denies read, update, delete, and execute permissions to a subset of roles defined in the **(Default)** ACD. (At your option, these roles can be defined in a specialized ACD, rather than the **(Default)** ACD.) In the illustration, ACLs for the Archive and Restore

Requests must grant run (execute) permission to roles expected to run these requests.

Archive File Security

A File Access Definition (FAD) defines the security rules for data in one or more Archive Files created by an Archive Request that references the FAD. The FAD in the diagram may grant access to archived data in selected tables and columns and deny access to data in others. The logon account used to run the Restore Request must be represented by a role in the FAD that is granted the necessary access to archived data.

Configure Security

To use ***Optim*** Security, you must initialize security for the ***Optim*** Directory, assign a Security Administrator, and enable the security features your site will use.

To initialize ***Optim*** Security and assign a Security Administrator, use one of the following **Tasks** menu options in the **Configuration** program:

- **Configure the First Workstation**
- **Configure Security for an Optim Directory**
- **Create/Update Optim Directory**
- **Configure Options**

To enable or disable the security features, select **Configure Security for an Optim Directory** from the **Tasks** menu in the **Configuration** program.

For more information, see **7.4 Configure Security for an Optim Directory** on page 192.

Chapter Contents

This chapter explains how to do the following:

- Create, edit, and maintain ACDs.
- Create roles.
- Define ACLs.
- Define FADs.

D.1 Access Control Domain

Use the **Access Control Domain Editor** to create and maintain Access Control Domains. There are different ways to open the editor depending upon whether you want to create a new Access Control Domain or select an Access Control Domain to edit.

Create a New ACD or Select an ACD to Edit

This section explains how to create or edit an Access Control Domain.

To create or edit an Access Control Domain:

1. In the main window, select **Access Control Domains** from the **Security** submenu on the **Options** menu to open the **Access Control Domains** dialog.
2. The next step depends on your purpose:
   - To create a new ACD, select **New ACD** from the **Tools** menu in the **Access Control Domains** dialog to open the **Access Control Domain Editor**.
   - To edit an existing ACD, double-click the grid row to display the desired ACD in the **Access Control Domain Editor**.
3. **Optional**. In the **Access Control Domain Editor**, right-click the **Role List** and select **New** or **Open** from the shortcut menu to open the **Role Specifications** dialog and define or edit roles in the **Role Specifications** dialog.
4. Save the role.
5. Save the ACD.
6. **Optional**. Edit the ACL for the ACD.
7. Click **OK** to save the ACD.

These steps are the minimum required to create an ACD. Refer to **D.1.1 Access Control Domain Editor** for complete details.

Access Control Domains List

The **Access Control Domains** dialog lists all ACDs in the ***Optim*** Directory. You must use this dialog to open the **Access Control Domain Editor** needed to create a new ACD or edit an existing ACD. From the **Access Control Domains** dialog, you can also list any FADs and ACLs that are based upon a listed ACD, which may be useful when maintaining ACDs. The list may help you to select an ACD to serve as the basis for a new FAD or ACL or to analyze the potential downstream effect of a change to the ACD. Also, from the list, you can display an

FAD or ACL to determine whether it references a role that should be included in the ACD.

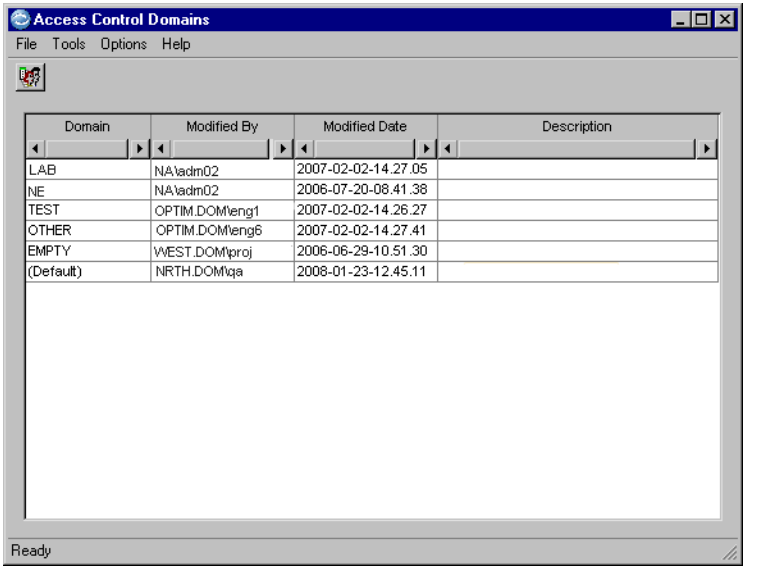
Each ***Optim*** Directory for which security is initialized contains an ACD named **(Default)**, which is the default ACD for secured objects in the directory. **(Default)** also determines the roles that can create and modify additional ACDs.

Permissions Needed to Create an ACD

To create an ACD, a user account must be a member of a role allowed the Create Access Control Domain privilege in the **(Default)** ACD. If Functional Security is not enabled, a user account must be a member of a role with update access to the ACL for the **(Default)** ACD.

Open Dialog

In the main window, select **Security** from the **Options** menu. Then select **Access Control Domains** from the submenu to open the **Access Control Domains** dialog.



The **Access Control Domains** dialog lists the ACDs in a read-only grid.

Domain The ACD name.

Modified By The identifier for the user account used to create or last modify the entry.

Modified Date The date and time the ACD was created or last modified.

Description Optional text that describes the ACD.

To open the **Access Control Domain Editor** and create a new ACD, click the **New ACD** toolbar button, select **New ACD** from the **Tools** menu, or use the shortcut menu. You can also use the shortcut menu to delete an ACD, list FADs and ACLs that are based upon the ACD, or open the ACL for the ACD.

Note: Access permissions in the ACL for the ACD determine the options and actions that are available to you. For example, the **Delete** shortcut menu option is not available to roles limited to read access.

Shortcut Menu Commands

Although similar to the Open dialog described in detail in the **Common Elements Manual**, the **Access Control Domains** dialog provides the following specialized shortcut menu commands:

New ACD Open the **Access Control Domain Editor** to create a new ACD.

Open Open the **Access Control Domain Editor** to view or edit the selected ACD.

Delete Delete the selected ACD from the ***Optim*** Directory. (Not available for the **(Default)** ACD.)

Note: When you delete an ACD, the **(Default)** ACD becomes the basis for any FADs or ACLs based upon the ACD. Roles that do not exist in the **(Default)** ACD are denied access.

List Object ACLs Open the **Open Object Access Control List** dialog, which lists the ACLs based upon the selected ACD.

This option is available only if the ACD is the basis for one or more ACLs. (Not available for the **(Default)** ACD.)

View or Edit ACD

To view or edit an ACD in the **Access Control Domain Editor**, double-click the grid row or select **Open** from the shortcut menu.

Note: Until network accounts are added to the ***Optim*** Administrator role or new roles are created in the **(Default)** ACD and granted Update access in the ACL, only the Security Administrator for the ***Optim*** Directory can edit **(Default)**.

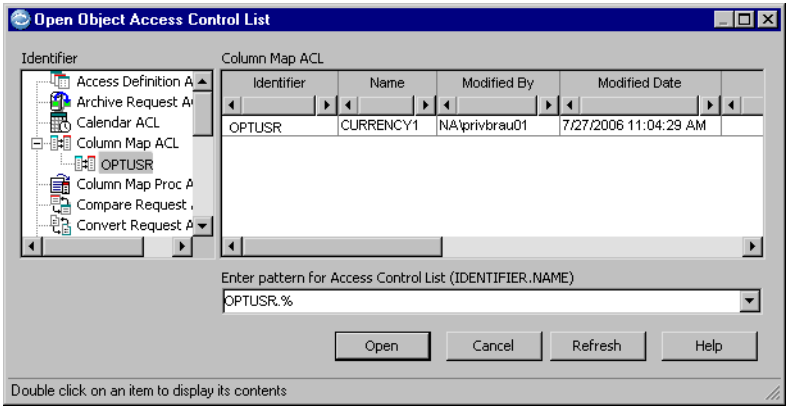
Create ACD

To create an Access Control Domain, a user must be a member of a role in the **(Default)** ACD, and:

- If Functional Security is not enabled, the user must be the Security Administrator or included in a role that has update access to the **(Default)** ACD.
- If Functional Security is enabled, the role must be allowed the Functional Privilege for Access Control Domains in the Create Security Definitions class.

Open Object Access Control List

Use the **Open Object Access Control List** dialog to list and display the ACLs associated with an ACD. Open this dialog by selecting **List Object ACLs** from the shortcut menu on the **Access Control Domains** dialog. This option is not available for the **(Default)** ACD. The **Open** dialog is discussed in detail in the **Common Elements Manual, 2.3 Using the Open Dialog**.

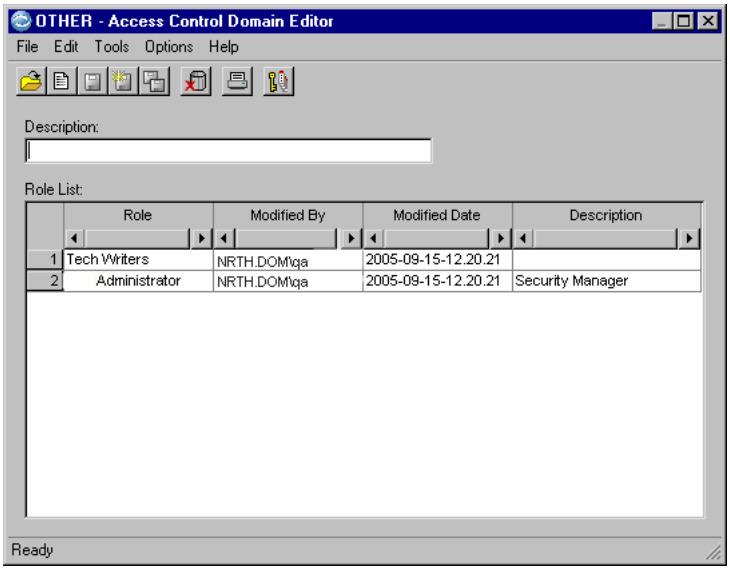


D.1.1 Access Control Domain Editor

The **Access Control Domain Editor** lists roles in the ACD. The name of the ACD is displayed at the top of the dialog. The **Role List** displays the roles in the ACD.

When you open the **Access Control Domain Editor** by selecting **New ACD** from the **Tools** menu in the **Access Control Domains** dialog, the ***Optim*** Administrator role is displayed by default. You can also open the **Access Control Domain Editor** dialog for an existing ACD by double-

clicking the name of an ACD listed in the **Access Control Domains** dialog.



To add, edit, or delete a role, use the shortcut menu to open the **Role Specifications** dialog, which is used to create and modify roles for an ACD and, if Functional or Object Security is used at your facility, to grant or deny related privileges to those roles.

Description Optional text that describes the ACD (up to 40 characters).

Role List A grid that displays the roles in the ACD and includes the following:

- **Role** The role name.
- **Modified By** The identifier for the user account used to create or last modify the entry.
- **Modified Date** The date and time the role was created or last modified.
- **Description** Text that describes the role.

Shortcut Menu

Right-click the **Role List** grid to display the following shortcut menu commands:

New Open the **Role Specifications** dialog to create a new role.

Open Open the **Role Specifications** dialog to view or edit the selected role.

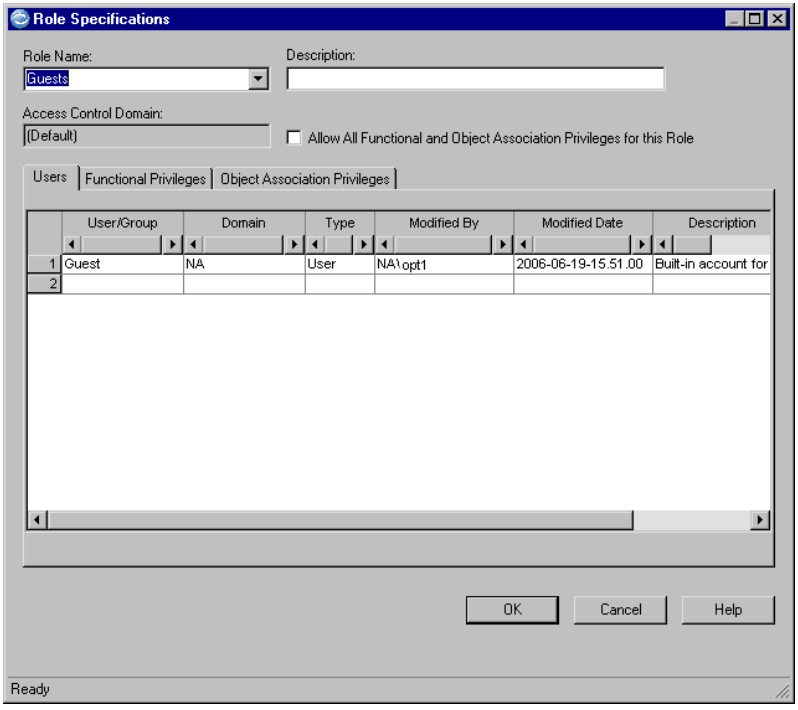
Delete Delete the selected role from the ACD. A confirmation prompt is displayed if Personal Options are set to provide it.

Note: The **Open** and **Delete** commands are not available for roles that are denied update access.

D.1.2 Role Specifications

The **Role Specifications** dialog allows you to create or edit a role within an ACD. From the dialog, you can identify the user and group accounts that are members of the role and assign access permissions. For roles in

the **(Default)** ACD, you can also grant or deny access to functions in ***Optim*** for a role.



Note: You must save the ACD in order to save any changes made to the role, including Functional or Object Association Privileges.

Role Name

The role name (up to 30 characters). To create a new role for the ACD, type the name or select from a history list of role name entries.

- You cannot use the **Role Name** history list to navigate from role to role in the ACD. You must open each role from the **Access Control Domain Editor**.
- It is possible to assign identical names to roles made up of different user accounts, if the roles are in different ACDs. For simplicity, a consistent naming convention that prevents duplicate role names may be advisable. However, duplicate role names may be useful if you wish to use the ***Optim*** Object Template ACL with more than one ACD. In this case, the Template ACL would assign access permissions to a standard set of roles with the role members varying by ACD.

You can use a role that is displayed in the **Role Specifications** dialog as a model to create a new role or replace another role in the ACD by typing or selecting a **Role Name** from the history list.

Description Optional text that describes the role (up to 40 characters).

Access Control Domain The ACD for the role.

Allow All Privileges for this Role Select the **Allow All Functional and Object Association Privileges** check box to allow the role all Functional (if editing the **(Default)** ACD) and Object Association Privileges. When this check box is selected, the **Allow All** and **Allow** check boxes are selected and cannot be cleared. Also, the **Allow All**, **Deny All**, and **Clear All** command buttons and the shortcut menus are unavailable. When the check box is cleared, the **Allow All** and **Allow** check boxes remain selected but can be cleared.

Tabs The **Role Specifications** dialog includes the following tabs:

Users The user and group accounts in the role.

Functional Privileges Access privileges to functions for accounts in the role.

Note: The **Functional Privileges** tab is available only from the **(Default)** ACD.

Object Association Privileges Permissions to use the ACD to secure ***Optim*** objects for accounts in the role.

D.1.3 Users Tab

Use the **Users** tab to add and delete user and group accounts in a role.

User/Group A user or group account from a network domain (up to 256 characters for users and up to 85 characters for groups).

Domain The network domain or UNIX node name that includes the user or group account.

Type Type of account. If entering the account manually, select the correct **Type** to validate the account.

Modified By The identifier for the user account used to create or last modify the entry.

Modified Date The date and time the account was created or last modified.

Description Text that describes the user or group account.

Shortcut Menu Commands Right-click the grid to display the following shortcut menu commands:

Add Users/Groups	Open the **Security Users and Groups** dialog, used to select multiple user and group accounts from a list of members in a network domain.
Remove	Remove the selected user or group account from the role.
Remove All	Remove all user and group accounts from the role.

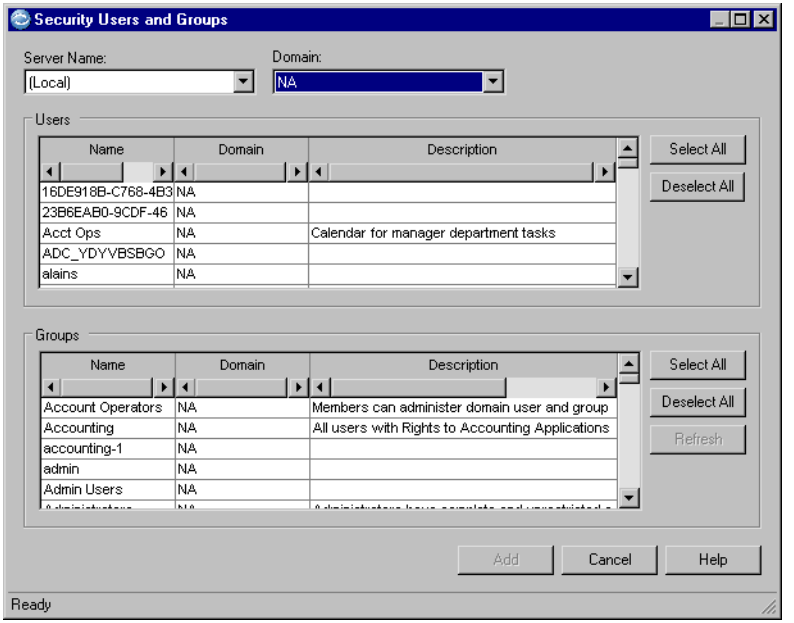
Everyone Group

The Everyone group includes all users in all Windows domains and UNIX nodes in your network. This group is not available in the **Security Users and Groups** dialog. To add this group to a role, type Everyone in **User/Group**, leave **Domain** blank, and select the **Type** Group.

Security Users and Groups

When you select **Add Users/Groups** from the shortcut menu on the **Users** tab, the **Security Users and Groups** dialog is displayed. Use the

Security Users and Groups dialog to select user and group accounts in a network domain.



Server Name

Select (Local) or the name of the ***Server*** with the domain connection appropriate for the account you want to add to the role. If your site does not use a ***Server***, (Local) is displayed and cannot be changed.

Domain

Select the name of the domain for the user and group accounts you want to add to the role. The domains are within a network that includes the designated **Server Name**.

Note: If the ***Server*** is on a UNIX platform, you do not need to specify a **Domain**. The node name is displayed in **Domain** at the top of the dialog and in the **Users** and **Groups** grids.

Users

The user accounts in the domain, including the **Name**, **Domain**, and **Description**.

Groups

The group accounts in the domain, including the **Name**, **Domain**, and **Description**.

Shortcut Menu Command

Right-click the **Users** grid to display the following shortcut menu command:

Display Groups for User Display only groups that include the selected user.

Command Buttons

The following command buttons are available on the **Security Users and Groups** dialog:

Select All Select all members in the grid.

Deselect All Clear all selections in the grid.

Refresh Redisplay all groups in the domain.

Add Add the selected users and groups to the role and open the **Role Specifications** dialog.

Cancel Return to the **Role Specifications** dialog without adding any users or groups to the role.

To list groups for a specific user, right-click the user name and select **Display Groups for User** from the shortcut menu. To redisplay all group accounts in the domain, click **Refresh**.

Select a single user or group account by clicking the name or select multiple user or group accounts by holding the **Ctrl** or **Shift** key while clicking the names. To select all accounts in a list, click **Select All**. To deselect all accounts in a list, click **Deselect All**. Click **Add** to add the selected accounts to the role and redisplay the **Role Specifications** dialog.

D.1.4 Privileges Tabs

Both the **Functional Privileges** tab and the **Object Association Privileges** tab are divided into two grids, one for privilege classes and the second for privileges that are included in the selected privilege class. If **Allow All Functional and Object Association Privileges** (for the **(Default)** ACD) or **Allow All Object Association Privileges for this Role** is selected, the role is granted all privileges in all privilege classes. To grant or deny selected privileges to a role, you must clear this option.

Assigning Privileges

By selecting **Allow All** or **Deny All** for a privilege class, you select corresponding check boxes for the associated privileges. For example, you can allow accounts in a role to secure action requests by selecting

Allow All for the Associate Action Editors Privilege Class on the **Object Association Privileges** tab. Accounts in the role can then secure an action request with an ACL that uses the ACD.

Note: You can define Functional Privileges from the **(Default)** ACD only.

Privilege Classes Grid

Use the Privilege Classes grid to display associated privileges in the Privileges grid. You can also use the Privilege Classes grid to allow or deny all privileges in either a single class or all classes.

To select a row in the Privilege Classes grid, click a row indicator cell or either an **Allow All** or **Deny All** cell. The grid arrow, ➔, indicates the class of privileges displayed.

You can also allow or deny all privileges in all privilege classes using the **Allow All** and **Deny All** buttons for the Privilege Classes grid or selecting corresponding commands from the shortcut menu. To remove all selections in the Privilege Classes grid, click or select **Clear All**.

Privileges Grid

Use the Privileges grid to allow or deny privileges within a privilege class. You can allow or deny a privilege by selecting the corresponding **Allow** or **Deny** check box. If both the **Allow** and **Deny** check boxes are cleared, the role is denied the privilege.

You can also allow or deny all privileges in the class using the **Allow All** and **Deny All** buttons for the Privileges grid or selecting corresponding commands from the shortcut menu. To remove all selections in the Privileges grid, click **Clear All**.

Users in Multiple Roles

When a user is a member of more than one role, the following rules apply to avoid security conflicts:

- If a privilege is denied for a role, then the privilege is unavailable to all members of the role, even the members associated with another role in which the privilege is allowed.
- If neither the **Allow** nor **Deny** check box in a **Privilege** tab is selected, the privilege is denied, but members of the role may be allowed the privilege as members of another role that is allowed the privilege.

Functional Privileges Tab

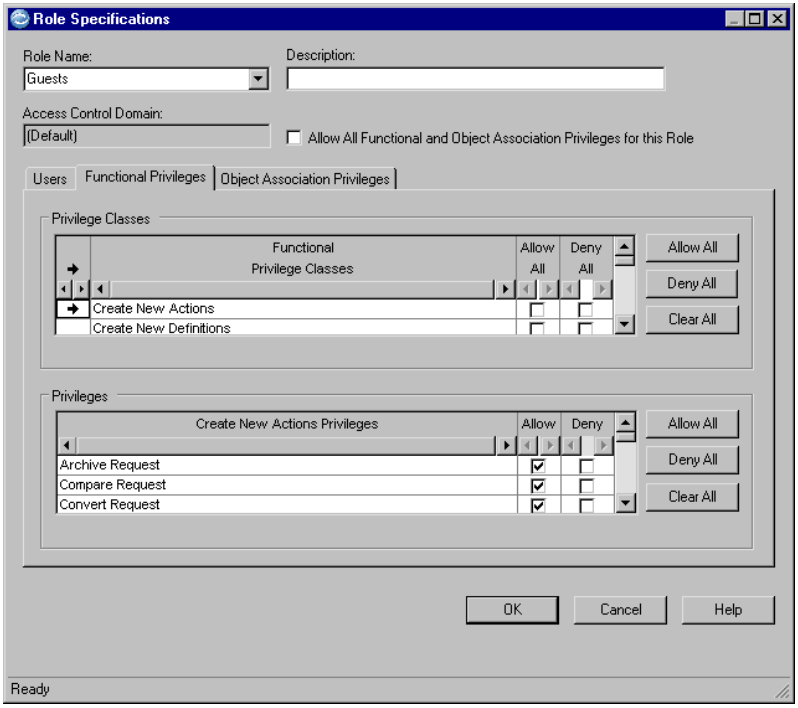
Use the **Functional Privileges** tab on the **Role Specifications** dialog to assign Functional Privileges to roles in the **(Default)** ACD. You can

allow or deny access to Functional Privileges for any role in the **(Default)** Access Control Domain. Configure Functional Security using the **Functional Privileges** tab on the **Role Specifications** dialog. For additional information, see **Assigning Privileges**.

When a role is denied a Functional Privilege, any functions associated with the privilege are unavailable to the user and group accounts in the role. For example, if the privilege to invoke the **Access Definition Editor** privilege from the **Invoke Definition Editors** privilege class is denied to a role, the **Access Definition** option in the **Definitions** menu on the main window is unavailable to users in that role and, also, the **Edit Access Definition** button and menu option are unavailable from any request editor (e.g., the **Extract Request Editor**).

The **(Default)** ACD governs Functional Privileges. Subordinate ACDs can determine Object Association Privileges only.

Important: Before Functional Security is first enabled, the Security Administrator must define Functional Privileges for all users. If Functional Privileges are not defined before Functional Security is enabled, users will be unable to access any functions in ***Optim***.



The Functional Privileges, by privilege class, are described below.

Create New Actions

Create New Actions privileges are required to create or make copies of action requests (e.g., an Archive Request). The **New** command and the ability to save a copy of a request in a respective request editor will be unavailable to roles that are denied a privilege.

(Local) privileges refer to requests that are created from another object editor. For example, if a role is denied the Insert Request (Local) privilege, the role will be unable to create a local Insert Request from the **Restore Request Editor**.

This class includes the following privileges:

Archive Request
Compare Request
Convert Request
Convert Request (Local)
Delete Request
Extract Request
Insert Request
Insert Request (Local)
Load Request
Load Request (Local)
Report Request
Report Request (Local)
Restore Request
Table Editor

Create New Definitions

Create New Definitions privileges are required to create or make copies of definitions (e.g., an Access Definition). The **New** command and the ability to save a copy of a definition in a respective definition editor will be unavailable to roles that are denied a privilege.

(Local) privileges refer to definitions that are created from another object editor. For example, if a role is denied the Access Definition (Local) privilege, the role will be unable to create a local Access Definition from the **Extract Request Editor**.

This class includes the following privileges:

Access Definition
Access Definition (Local)
Column Map
Column Map (Local)
Column Map Proc(edure)
Column Map Proc (Local)
***Optim* Primary Key**
***Optim* Relationship**
Table Map
Table Map (Local)

Create Security Definitions

Create Security Definitions privileges are required to create or make copies of security definitions (e.g., an Access Control Domain). The **New** command and the ability to save a copy of a security definition in a respective security definition editor will be unavailable to roles that are denied a privilege.

This class includes the following privileges:

Access Control Domain
File Access Definition

Create Utility Definitions

Create Utility Definitions privileges are required to create or make copies of utility definitions (e.g., a Storage Profile). The **New** command and the ability to save a copy of a utility definition in a respective utility editor will be unavailable to roles that are denied a privilege.

This class includes the following privileges:

Calendar
Archive File Collection
Currency
Storage Profile

Editor Options

Editor Options privileges are required to create database objects (e.g., create tables, drop tables, or modify SQL statements).

This class includes the following privileges:

Create Indexes During Primary Key Index Analysis

Create Indexes During Primary Key Index Analysis privilege is required to create new indexes from the **Primary Key Index Analysis** dialog.

Create Indexes During Relationship Index Analysis

Create Indexes During Relationship Index Analysis privilege is required to create new indexes from the **Relationship Index Analysis** dialog.

Create Tables During Create

Create Tables During Create privilege is required to create new tables during the Create Process.

	Drop Tables During Create	Drop Tables During Create privilege is required to drop tables during the Create Process.
	Modify SQL During Create	Modify SQL During Create privilege is required to modify SQL statements during the Create Process.
	Modify SQL During Primary Key Index Analysis	Modify SQL During Primary Key Index Analysis privilege is required to modify SQL statements when creating indexes from the **Primary Key Index Analysis** dialog.
	Modify SQL During Relationship Index Analysis	Modify SQL During Relationship Index Analysis privilege is required to modify SQL statements when creating indexes from the **Relationship Index Analysis** dialog.
File Maintenance	File Maintenance privileges are required to delete or rename files and directories.	
	This class includes the following privileges:	
	File Deletion	Delete a file or directory.
	File Renaming	Rename a file or directory.
Invoke Action Editors	Invoke Action Editors privileges are required to create, edit, or run an action request (e.g., Insert Request). The respective **Action** menu item will be unavailable to roles that are denied a privilege.	
	This class includes the following privileges:	

Archive Request	**Insert Request**
Compare Request	**Load Request**
Convert Request	**Report Request**
Delete Request	**Restore Request**
Extract Request	**Table Editor**

Invoke Command Line Actions

Invoke Command Line Actions (PR0CMND) privileges are required to execute a utility from the command line.

This class includes the following privileges:

Archive Directory Maintenance	Invoke Archive Directory Maintenance privilege is required to register or unregister Archive Files or update Archive File entries from the command line (i.e., use /ARCMAINT).
Browse	Invoke Browse privilege is required to browse Archive Files, Compare Files, Extract Files, and Control Files from the command line (i.e., use /X).
Import	Invoke Import privilege is required to import ***Optim*** objects from the command line (i.e., use /IMPORT).
Migrate	Invoke Migrate privilege is required to perform the Archive File Migration Process (i.e., use /MIGRATE).
Restart/Retry	Invoke Restart/Retry privilege is required to restart or retry processes from the command line (i.e., use /RESTARTRETRY).
Run	Invoke Run privilege is required to run processes from the command line (i.e., use /R).
Table Editor	Invoke Table Editor privilege is required to edit tables from the command line (i.e., use /E).

Invoke Configuration Actions

Invoke Configuration Actions privileges are required to perform tasks within the **Configuration** program (e.g., **Create/Update DB Alias**). The respective **Tasks** menu item will be unavailable to roles that are denied a privilege.

This class includes the following privileges:

Apply Maintenance for DB Alias
Create/Update DB Alias
Drop Optim Directory/DB Alias
Update DBMS Version for DB Alias

Invoke Definition Editors

Invoke Definition Editor privileges are required to create or edit an ***Optim*** object (e.g., an Access Definition). The respective **Definitions** menu item will be unavailable to roles that are denied a privilege.

This class includes the following privileges:

Access Definition	**Point and Shoot**
Column Map	**Primary Key**
Column Map Proc(edure)	**Relationship**
DB Alias	**Table Map**

Invoke Options

Invoke Options privileges are required to edit Product Options or use dialogs for securing ***Optim*** functions, objects, and Archive Files. The respective **Options** menu item will be unavailable to roles that are denied a privilege.

This class includes the following privileges:

Access Control Domain
Export Security Definitions
File Access Definition
Import Security Definitions
Product Options

Invoke Utilities

Invoke Utilities privileges are required to open the utilities dialogs. The respective **Utilities** menu item will be unavailable to roles that are denied a privilege.

This class includes the following privileges:

Archive Directory Maintenance	Invoke Archive Directory Maintenance privilege is required for roles that maintain Archive Files or the Archive Directory.
Archive Index Maintenance	Invoke Archive Index Maintenance privilege is required for roles that maintain Archive Indexes.

Browse	Invoke Browse privilege is required for roles that browse Archive, Compare, Extract, or Control Files.
Calendar	Invoke Calendar privilege is required for roles that create or edit Calendars.
Create	Invoke Create privilege is required for roles that create database objects, either online or from the command line.
Currency	Invoke Currency privilege is required for roles that create or edit Currency Definitions.
Export	Invoke Export privilege is required for roles that export ***Optim*** objects.
Import	Invoke Import privilege is required for roles that import ***Optim*** objects.
Register Archive File	Invoke Register Archive File privilege is required for roles that register Archive Files, whether online or from the command line.
Restart/Retry	Invoke Restart/Retry privilege is required to restart or retry a process.
Scheduling Editor	Invoke Scheduling Editor privilege is required to schedule process requests.
Storage Profile	Invoke Storage Profile privilege is required to manage archive media.
Archive File Collection	Invoke Archive File Collection privilege is required for roles that create or edit Archive File Collections, used with Open Data Manager.

Run Untitled Actions

Run Untitled Actions privileges are required to process new action requests not saved prior to processing (i.e., requests for which Untitled is displayed in the dialog heading). The **Run** command in a respective action editor will be unavailable to roles that are denied a privilege.

This class includes the following privileges:

Archive Request	**Insert Request**
Compare Request	**Load Request**
Convert Request	**Report Request**
Delete Request	**Restore Request**
Extract Request	

Security Tasks

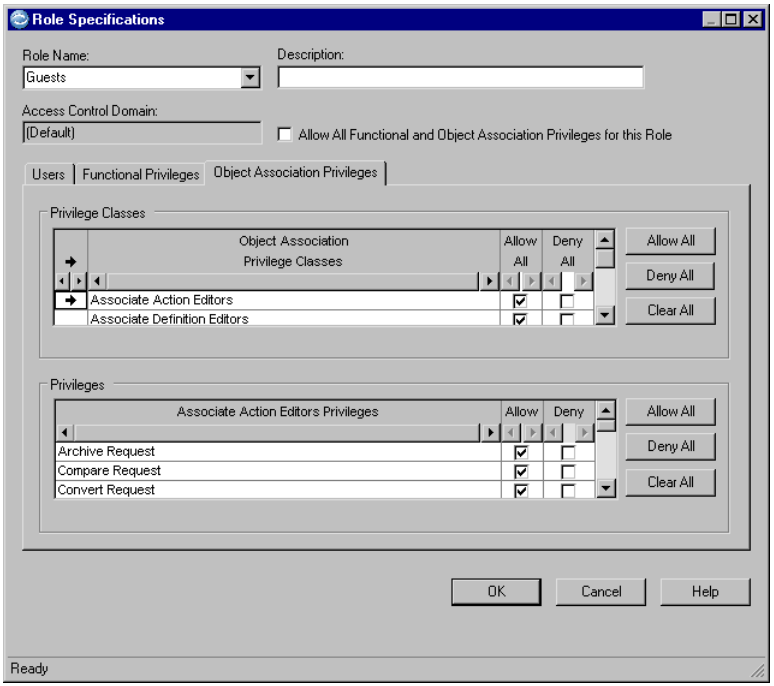
Security Tasks privileges are required to export or import secured Archive Files, modify a FAD, or run a Security Report.

This class includes the following privileges:

Export Secured Archive File	Export a secured Archive File.
Import Secured Archive File	Import a secured Archive File.
Modify File Security with Migrate	Use the Archive File Migration Process to change a FAD.
Report Security Privileges	Run a Security Report.

Object Association Privileges Tab

Use the **Object Association Privileges** tab to indicate the types of object for which the role will have Object Association Privileges. Object Association Privileges allow the role to use roles defined in the the ACD as the basis for an ACL that protects objects of the indicated type.



For more information about working with privileges and privilege classes, see **Assigning Privileges**.

Associate Action Editors

Associate Action Editors privileges are required to associate the ACD with an ACL that secures an Action request, which is created in a editor selected from the **Actions** menu. For example, an Archive File Request.

This class includes the following privileges:

Archive Request	**Insert Request**
Compare Request	**Load Request**
Convert Request	**Report Request**
Delete Request	**Restore Request**
Extract Request	**Table Editor**

Associate Definition Editors

Associate Definition Editors privileges are required to associate the ACD with an ACL that secures a Definition, which is created in an editor selected from the **Definitions** menu. For example, an Access Definition Request.

This class includes the following privileges:

Access Definition	**Point and Shoot**
Column Map	**Primary Key**
Column Map Proc(edure)	**Relationship**
DB Alias	**Table Map**

Associate Utilities

Associate Utilities privileges are required to associate the ACD with an ACL that secures a Utilities object, which is created in an editor selected from the **Utilities** menu. For example, a Currency Definition Request.

This class includes the following privileges:

Calendar	**Currency**
Archive File Collection	**Storage Profile**

D.2 Access Control List

An Access Control List (ACL) governs the ability of a role to perform actions (such as read, update, or delete) on both an object and the associated ACL. Each Access Control Domain, File Access Definition, and secured ***Optim*** object has an ACL. (Note that ACLs for objects other than security definitions have no effect unless the Security Administrator has enabled Object Security.)

When you secure an object, access to any associated Local objects is governed by the ACL for the parent object. Local objects are not secured individually; they are secured with the object in which they are embedded.

Use the **Access Control List Editor** to set access permissions for an object and the associated ACL. In general, an ACL is based upon a specific ACD, which defines the roles referenced by the ACL. Roles that are not in the ACD or not included in the ACL are denied all access to the object and ACL. However, the owner of the ACL always retains full access to the ACL, regardless of permissions granted or denied by the ACL.

Object Association Privileges

In order to create an ACL when Functional Security is enabled, a user must be a member of a role to which the ACD grants Object Association Privileges for the object type. Object Association Privileges are defined on the **Object Association Privileges** tab in the **Role Specifications** dialog. Use the tab to identify object types that the role can use with the ACD. For more information about defining Object Association Privileges, see **Object Association Privileges Tab**.

Automatically Associate an Object with an ACL

The ACL for a security definition (ACD or FAD) is created automatically at the time the definition is saved. ACLs for other objects may be created automatically, at the time the object is created and saved, or manually. Automatically created ACLs can be edited at any time by an authorized user.

The initial ACL for a security definition references a ***Optim*** Administrator role for the owner and grants full access to the ACL for that role. The initial ACL for other objects is modeled after the ***Optim*** Object Template ACL, if one was created at the time ***Optim*** Security was configured for your installation. If the ***Optim*** Object Template ACL does not exist or the owner of the object is not granted object association privilege for the ACD that forms the basis for the Template ACL, the owner (creator) of the object is prompted to define the required ACL.

Note: Only the Security Administrator can define the ***Optim*** Object Template ACL, using the **Configuration** Program or selecting from the **Security** submenu to the **Options** menu in the main window. See **7.4.4 Set Optim Object Security Option** on page 197 for further information.

Manually Associate an Object With an ACL

You can create an ACL manually by selecting **Edit ACL** from either the **Tools** menu in the object editor or the shortcut menu in the **Open** dialog to display the **Access Control List Editor**. You can also use these options to edit an ACL. Settings in the ***Optim*** Object Template ACL, if the Template ACL exists, are used to populate the **Access Control List Editor**. If there is no ***Optim*** Object Template ACL, the editor is blank.

Remove an ACL

You cannot delete the ACL for an object for which security is required. To delete an ACL, you must be the ACL owner or in a role that is allowed Delete permission for the ACL. To remove the ACL for an object, select **Delete ACL** from the **Tools** menu in an object editor, or right-click the object name in the **Open** dialog and select **Delete ACL** from the shortcut menu. You can also click **Delete** on the **Access Control List Editor**.

Create or Edit an ACL

This section explains how to create or edit an Access Control List.

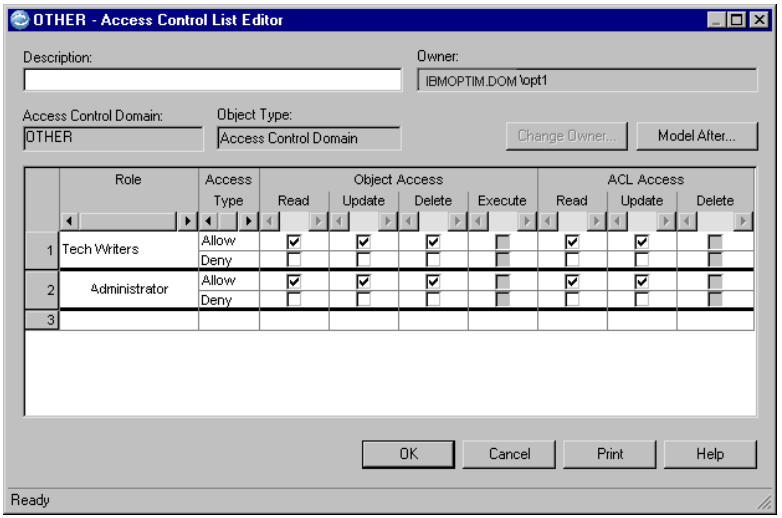
To create or edit an Access Control List:

1. In the object editor, select **Edit ACL** from the **Tools** menu to open the **Access Control List Editor**.
2. The next step depends on your purpose:
   - To change the ACD used as the basis for roles listed in the ACL, select a name from the **Access Control Domain** drop-down list.
   - To select an existing ACL to use as a model for the ACL displayed in the **Access Control List Editor**, click the **Model After** button to display the **Select Access Control List Model** dialog.
   - To list a Role, select a role name from the **Role** drop-down list in the grid.
   - To **Allow** or **Deny** access to the object or associated ACL, select the appropriate check boxes.
3. Click **OK** to save the ACL and redisplay the object editor.

These steps are the minimum required to create or edit an ACL. Refer to the following for complete details.

D.2.1 Access Control List Editor

Use the **Access Control List Editor** to define access permissions for an object and the associated ACL.



Note: Access permissions in the ACL determine the options and actions that are available to you. For example, the **Remove** shortcut menu options are not available to roles limited to read access.

Description Enter text that describes the ACL (up to 40 characters).

Owner The user account with all access rights to the ACL. The owner can always read, update, or delete the ACL even if the account is included in a role that is denied access to these actions. To change the owner, click **Change Owner**.

Note: The Security Administrator is the owner of the **(Default)** ACL and ***Optim*** Object Template ACL.

Access Control Domain The ACD that forms the basis for the roles in the ACL. An ACL references roles in the ACD in order to translate them into network accounts. Roles not defined in the ACD, or in the ACD but not referenced in the ACL, are denied access.

Object Type The type of object secured by the ACL.

ACL Grid

The grid allows you to list roles in the ACL and define permissions.

Role

Enter a role name or select from the drop-down list of roles in the ACD. Role names not included in the ACD are italicized.

Notes:

- If the ACD does not include any roles, the **Role** list is not available.
- A role that is not defined in the ACD is denied all access.
- A user or group account that is not included in a listed role is denied all access.
- The most restrictive permission applies to a user or group account that is included in multiple roles in the ACL.

Access Type

Allow and **Deny** identify the check boxes in their rows. If both the **Allow** and **Deny** check boxes are cleared, accounts in the role are provisionally denied the privilege but may be granted the privilege as members of another role.

Object Access

Possible access to the object. Use each set of **Allow** and **Deny** check boxes to define access permissions for the role.

Read

Controls the ability to open or view an object. If access is denied, a warning popup indicates the object is restricted by security.

A role must have Read access, in addition to Update access, to the object in order to update the object.

Update

Controls the ability to save an object. If access is denied, the **Save** command will not be available from the object editor.

Note: Roles denied update access can use the **Save As** command to rename an object.

Delete Controls the ability to delete an object. If access is denied, the **Delete** command is not available from the object editor and the **Open** dialog.

Execute Controls the ability to run a process. This option is available only for objects created with editors listed in the **Actions** menu. If access is denied, the **Run** command is not available from the Request Editor and the **Execute** command is not available from the **Table Editor**.

ACL Access Possible access to the ACL. Use each set of **Allow** and **Deny** check boxes to define access permissions for the role. If both the **Allow** and **Deny** check boxes are cleared, accounts in the role are provisionally denied the privilege but may be granted the privilege as members of another role.

Read Controls the ability to view the ACL. A role must have Read access, in addition to Update access, to the ACL in order to update the ACL.

Update Controls the ability to modify the ACL.

Delete Controls the ability to delete the ACL. Not available for ACDs or File Access Definitions or for ***Optim*** objects that are secured automatically when saved.

Shortcut Menu Commands

Right-click the grid to display the following shortcut menu commands:

Remove Remove the selected role from the ACL.

Remove All Remove all roles from the ACL.

Allow All Allow all Object Access, ACL Access, or both to the role.

Deny All Deny all Object Access, ACL Access, or both to the role.

Clear All Allowed For the role, clear all **Allow** check boxes for Object Access, ACL Access, or both.

Clear All Denied For the role, clear all **Deny** check boxes for Object Access, ACL Access, or both.

Right-click the grid column for an action to display the following shortcut menu commands:

Allow All *action* Access Allow access to all roles for the selected action.

Clear All *action* Access Clear all **Allow** and **Deny** check boxes for all roles for the selected action.

Deny All *action* Access Deny access to all roles for the selected action.

Command Buttons

The following command buttons are available on the **Access Control List Editor**:

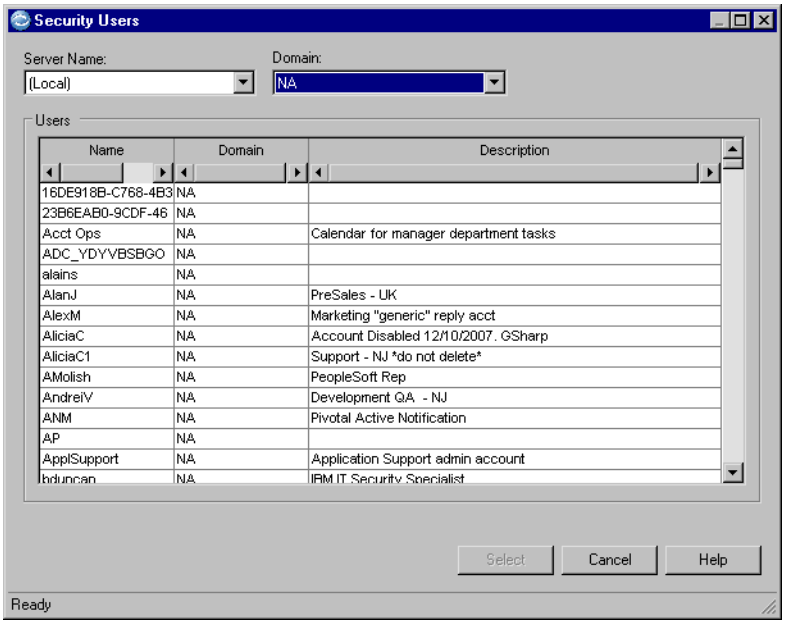
Change Owner Open the **Security Users** dialog to assign ACL ownership to another user account. Available to user accounts permitted to update the ACL who are also the ACL owner or the Security Administrator for the ***Optim*** Directory. For more information about this dialog, see **Security Users**.

Note: **Change Owner** is not available for the **(Default)** ACL and the ***Optim*** Object Template ACL.

Model After Open the **Select Access Control List Model** dialog to model the ACL after another ACL. Available to roles permitted to update the ACL. For more information about this dialog, see **Select Access Control List Model**.

Security Users

Click **Change Owner** to open the **Security Users** dialog, used to reassign ACL ownership. Use this dialog to select a user account from a list of accounts in a specified network domain. To display the list, select an ***Optim*** **Server Name** and a **Domain**. To select a network user account, click the name in the **Users** grid, and click **Select**.



Server Name Select the name of a ***Server***. If your site does not use a ***Server***, (Local) is displayed.

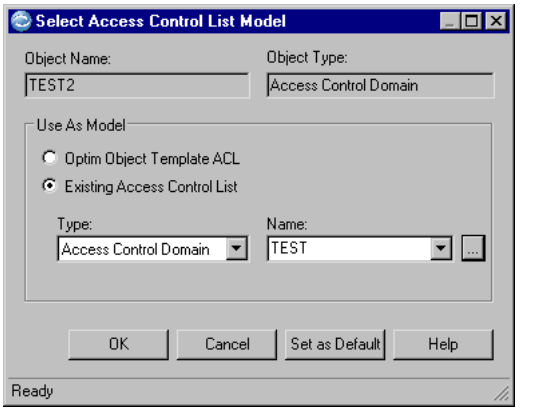
Domain Select the name of the domain for the users you want to list. The domain is within a network that includes the server in **Server Name**.

Note: If a UNIX server is selected, the node name is displayed in **Domain** and in the **Users** grid.

Users A list of user accounts by **Name**, with **Domain** and a **Description**.

Select Access Control List Model

To model an ACL after the ACL for another security definition or ***Optim*** object, click **Model After** to open the **Select Access Control List Model** dialog.



To select an ACL as a model, enter the object **Type** and **Name**. To apply the ACL for the selected object as a model, click **OK**. The roles and permissions from the model are then displayed in the **Access Control List Editor**.

Object Name Name of the object with the model ACL.

Object Type Type of object with the model ACL.

Use As Model Select an ACL to use as a model, using the following:

Optim Object Template ACL	Option to use the Optim Object Template ACL as the model.
Existing Access Control List	Option to use the ACL as the model **Type** and **Name**.
Type	Select the object type associated with the model ACL.

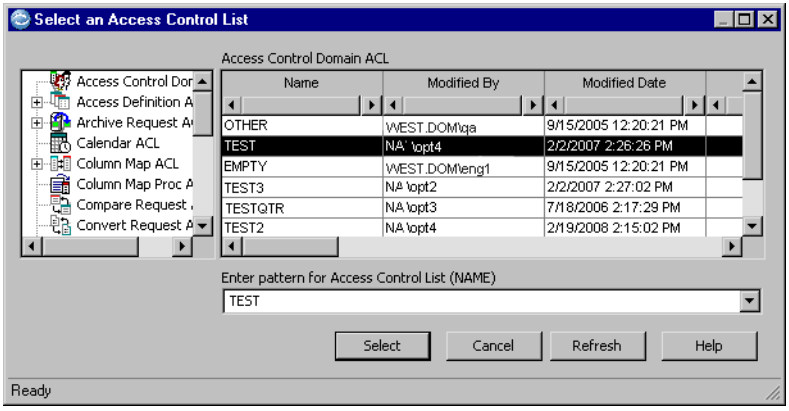
Name Type or select the object name associated with the model ACL.

You can also use the **Name** browse button to open the **Select an Access Control List** dialog, used to select a model ACL from a list of objects. If you select an ACL using the **Select an Access Control List** dialog, the **Type** and **Name** for the selected ACL will be displayed automatically.

To populate **Type** and **Name** with the current entries each time you open the **Select Access Control List Model** dialog, click **Set as Default**.

Select an Access Control List

Use the **Select an Access Control List** dialog to select a model ACL from a list of objects. The **Identifier** area displays the object types to list on the right side of the dialog.



After you select an **Identifier**, ACLs are listed on the right side, below the type of object. Double-click the desired ACL to select it as a model.

Note: An ACL is identified by the name of its associated object.

Enter Pattern for Access Control List allows you to limit the ACL list to names that match the specified criteria. You can use the % (percent) wild card to represent one or more characters, or use the _ (underscore) wild card to represent a single character. (The underscore must be selected as the SQL LIKE character on the **General** tab of Personal Options.) After you specify a **Pattern**, click **Refresh** to redisplay the list based on your criteria.

D.3 File Access Definition

Use a File Access Definition to control access to data in one or more Archive Files created by running an Archive Request that references the FAD. The archived data is protected according to the settings in the FAD, which can be changed as the security requirements for your site change. When settings in the FAD are changed, the changes apply to the previously archived data as well as to data archived in the future.

A File Access Definition allows you to control access to data in specified tables and columns, or use a default setting to control access to tables and columns for which access is not granted explicitly. You can define access permissions by creating an access list for a table, column, or the default. All users are allowed unlimited access to archived data to which an access list does not apply. File Access Definition specifications for tables and columns that do not exist in an associated Archive File do not affect the security of the file.

Only roles in the Access Control Domain (ACD) used as the basis for the File Access Definition can be assigned explicit permissions. Any user accounts for which explicit permissions do not apply are allowed or denied access according to a default setting for the File Access Definition.

For example, you can grant access to roles in the ACD explicitly and use the default setting to deny access to all other users. For a detailed File Access Definition example, see **D.3.3 File Access Definition Example**.

Permissions Needed to Create an FAD

To create an FAD, a user account must be a member of a role allowed the Create File Access Definition privilege in the **(Default)** ACD. If Functional Security is not enabled, a user account must be a member of a role with update access to the ACL for the **(Default)** ACD.

Using Secured Archive Files

You can limit the ability of roles to process or view archived data at the level of table or column. For a Restore Process, members of a role can insert or update from a table and column in a secured Archive File, if permitted. If the account is not permitted to access a column that affects the referential integrity of the data, e.g., a primary key, an error message is displayed in the Process Report.

For a Delete Process, only an account that is permitted access to data in a table and column in a secured Archive File can delete database data from that table and column. If an account is not permitted to access a column that affects the referential integrity of the data, e.g., a primary key, an error message is displayed in the Process Report.

For a Browse session, an account must be permitted access to data in a table and column in a secured Archive File in order to browse the data.

Accounts that are denied access to data in all tables or columns in a secured Archive File cannot use the file in any ***Archive*** process or Browse session. A message indicates that the file cannot be opened. If an Archive File is associated with a File Access Definition that does not exist, the file cannot be used to define or run a process.

Registering Secured Archive Files

A secured Archive File must have an accompanying Security File in order to be registered. Using the **Archive Directory Maintenance** dialog, you can export the security information for an Archive File into a Security File. The Security File protects the Archive File by requiring a password to register the Archive File.

During registration, the secured Archive File is associated with a new or existing File Access Definition in the target ***Optim*** Directory. For more information about registering Archive Files and the **Archive Directory Maintenance** dialog, refer to the ***Archive*** **User Manual, Chapter 9. Archive Maintenance Utilities**.

Use the **File Access Definition Editor** to create and maintain File Access Definitions. You can open the ACL for a File Access Definition from this dialog or from the **File Access Definitions** dialog.

Create or Edit an FAD

This section explains how to create or edit a File Access Definition.

To create or edit a File Access Definition:

1. In the main window, select **File Access Definitions** from the **Security** submenu on the **Options** menu to open the **File Access Definitions** dialog.
2. The next step depends on your purpose:
   - To create a new FAD, select **New FAD** from the **Tools** menu in the **File Access Definitions** dialog to open the **File Access Definition Editor**.
   - To edit an existing FAD, double-click the grid row to display the desired FAD in the **File Access Definition Editor**.
3. The next step depends on your purpose:
   - To change the ACD used as the basis for roles listed in a new FAD, select a name from the **Access Control Domain** drop-down list.
   - To edit the **Table List** or list columns for explicit permissions, use the shortcut menu.
   - To list a Role, select a role name from the **Role** drop-down list in the Table Access Control grid.

- To **Allow** or **Deny** access to the table or column, select the appropriate check boxes.

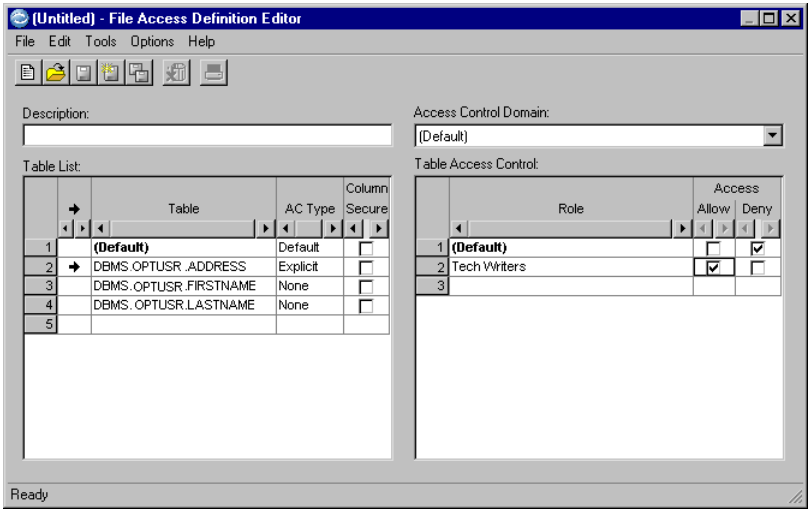
4. Click **OK** to save the FAD.

These steps are the minimum required to create or edit an FAD. Refer to the following for complete details.

D.3.1 File Access Definition Editor

Use the **File Access Definition Editor** to define a File Access Definition. This dialog allows you to select an **Access Control Domain** to be used as the basis for the File Access Definition, select tables to secure using the **Table List**, and define access permissions for each selected table using the **Table Access Control** list. You can also define access permissions for columns in a listed table.

Open the **File Access Definition Editor** by selecting **New FAD** from the **Tools** menu in the **File Access Definitions** dialog. You can also open that Editor for an existing File Access Definition by double-clicking a listing in the **File Access Definitions** dialog.



Description Enter text that describes the File Access Definition.

Access Control Domain Type or select the name of an Access Control Domain (ACD) to use as the basis for the File Access Definition. The ACD translates the roles specified in the **Table Access Control** list into accounts in your

network. After a File Access Definition is saved, you can select a different ACD by modifying the associated ACL.

Table List

(Default) and names of tables for which the File Access Definition explicitly controls access. Select an entry in the list to display or define corresponding access permissions in the **Table Access Control** list. The **(Default)** setting applies to archived data in tables not otherwise listed and cannot be deleted.

➔ Identifies the active entry; to select an entry, click the row.

Table The fully qualified table name. You cannot save a File Access Definition if any table name is not fully qualified.

Type the fully qualified three-part name, or use **Add table** from the shortcut menu to select a table name from a database or an Archive File. To remove a table name, select the row number and press **Delete** or use the **Remove** commands in the shortcut menu.

Any security settings for tables or columns that are not in the secured Archive File have no effect.

AC Type The type of access permissions associated with the table. Access permissions are displayed in the **Table Access Control** list. Select one of the following:

Explicit Table-specific access permissions apply.

Default The access permissions for **(Default)** apply.

None Access permissions do not apply. All users are allowed to access the table.

Notes: If **AC Type** is None:

- The **Column Secured** check box and **Table Access Control** list are unavailable and any user account is allowed full access.
- If for **(Default)**, the Default **AC Type** is unavailable for other entries in the **Table List**.

Column Secured Indicator that access permissions are defined for one or more columns in the table.

To define access permissions for columns, right-click the table entry and select **List Columns** from the shortcut menu. Column access permissions are defined in the **Table Access Control** dialog. **Column Secured** indicates a table with column access permissions defined.

Shortcut Menu Commands

Right-click a row in the **Table List** to display the following shortcut menu commands:

Remove Table — Remove the table name from the list. This command is not available for **(Default)**.

Remove All Tables — Remove all table names, except **(Default)**, from the list.

List Columns — Open the **Table Access Control** dialog to define access permissions for columns in the selected table. This command is not available for **(Default)**.

Add table — Display submenus and select a source, **From Database** or **From Archive File**, for a table selection list. Use the list to add one or more table names to the **Table List**.

Note: **Add table** is available only from the blank row at the bottom of the **Table List**.

Select **From Database** to display the **Select Table(s)** dialog listing tables in the database. For more information, see **Selecting Tables from a Database**.

Select **From Archive File** to display the **Open** dialog, from which to choose an Archive File before displaying the **File Access Definition Table/Column Selection** dialog. For more information, see **Selecting Tables from an Archive File**.

Note: Access permissions in the ACL for the FAD determine the options and actions that are available to you. For example, the **Remove** shortcut menu options are not available to a role that is limited to read access.

Table Access Control

Use the **Table Access Control** list to define access permissions for an entry in the **Table List**. You can assign access permissions to selected roles in the associated ACD and a default for all user accounts and roles for which access permissions are not assigned explicitly. If the **AC Type** for an entry in the **Table List** is None, **Table Access Control** list is blank and cannot be edited.

Role **(Default)** and names of roles for which the File Access Definition explicitly controls access. Role names not included in the Access Control Domain that serves as the basis for the FAD are italicized and settings for them have no effect.

Notes:

- If a user is included in multiple roles in the list, the most restrictive permission applies.
- Unless the **AC Type** for the Table List entry is None, the **Table Access Control** list includes a **(Default)** setting. This default cannot be deleted and applies to users for which no explicit permissions are granted.

Type the name, or use the drop-down list to select the name of a role defined in the ACD. You can also edit a role name. To remove a role name, use the **Remove** commands in the shortcut menu.

Access The type of access permissions for the role. Select one of the following:

Allow The role is allowed access to the table.

Deny The role is denied access to the table.

You must select either **Allow** or **Deny** for **(Default)**. Roles for which both **Allow** and **Deny** are blank assume the permission selected for **(Default)**.

Shortcut Menu Commands

Right-click the **Table Access Control** list to display the following shortcut menu commands:

Remove	Remove the role from the list. This command is not available for **(Default)**.
Remove All	Remove all roles, except **(Default)**, from the list.
Allow all non-default	Allow access for all listed roles, except **(Default)**.
Deny all non-default	Deny access for all listed roles, except **(Default)**.

Selecting Tables from a Database

Use the **Select Table(s)** dialog to select the names of one or more tables from a database referenced by a specified DB Alias. To open the **Select Table(s)** dialog, right-click the blank row at the bottom of the Table List, select **Add table** from the shortcut menu, and select **From Database** from the submenu. You can then select one or more table names to be added to the **Table List**.

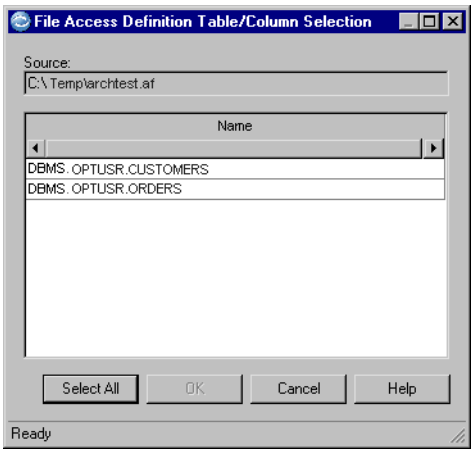
The **Select Table(s)** dialog lists the database tables:

- DB Aliases for available databases are listed on the left. To list tables in a database, double-click the DB Alias or overtype the DB Alias in the **Pattern** box.
- Objects referenced by the selected DB Alias are listed in the **Database Table** grid in alphabetical order by Creator ID and Table Name. The type of object (table, view, alias, synonym), DBMS, and fully qualified name are provided.

Selecting Tables from an Archive File

When you select **Add table** from the **Table List** shortcut menu, and select **From Archive File** from the submenu, the **Open** dialog is displayed to allow you to select an Archive File.

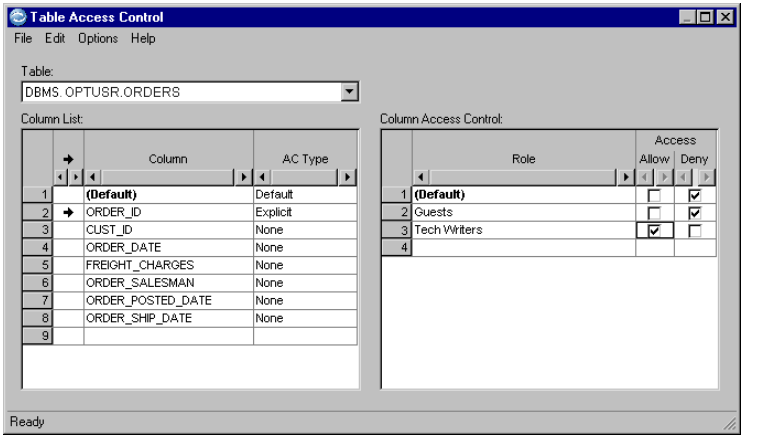
In the **Open** dialog, select the server on which the file resides and click **Refresh**. Use **Look In** to select the directory or path containing the file, and then double-click a listed file **Name** or enter the **File Name** and click **Open**. The names of tables in the selected file are listed in the **File Access Definition Table/Column Selection** dialog. **Source** indicates the path for the file.



Use the **File Access Definition Table/Column Selection** dialog to select the names of one or more tables in the Archive File. Click a table name to select it. To select multiple tables, hold the **Ctrl** or **Shift** key while clicking the table names. To select names of all tables in the Archive File, click **Select All**. Click **OK** to add the selected names to the **Table List** and re-display the **File Access Definition Editor**.

D.3.2 Defining Access Permissions for Columns

Permissions for columns are defined using a method similar to that for tables. To define access permissions for one or more columns in a table, right-click the table name on the **Table List** and select **List Columns** from the shortcut menu. The **Table Access Control** dialog is displayed.



Table

The table for which column access permissions are defined. Use **Table** to select other names from the **Table List** in the **File Access Definition Editor** and define column access permissions.

Column List

(Default) and names of columns in the **Table** for which the File Access Definition explicitly controls access. Select an entry in the list to display or define corresponding access permissions in the **Column Access Control** list. The **(Default)** setting applies to archived data in columns not otherwise listed and cannot be deleted.

➔	The arrow indicates the active entry. To select an entry, click the row.
Column	The column name. Type the name, or use **Add column** from the shortcut menu to select a column name from a database or an Archive File. To remove a column name, select the row number and press **Delete** or use the **Remove** commands in the shortcut menu. Any security settings for tables or columns that are not in the secured Archive File have no effect.

AC Type The type of access permissions associated with the column. Access permissions are displayed in the **Column Access Control** list.

Select one of the following:

Explicit Column-specific access permissions apply.

Default The default access permissions apply.

None Access permissions do not apply. All users are allowed to access the table.

Notes: If **AC Type** is None,

- The **Column Access Control** list is unavailable and any user account is allowed full access.
- If for **(Default)**, the Default **AC Type** is unavailable for other entries in the **Column List**.

Shortcut Menu Commands

Right-click a row in **Column List** to display the following shortcut menu commands:

Remove Column — Remove the selected column name from the list. (This command is not available for **(Default)**.)

Remove All Columns — Remove all column names, except **(Default)**, from the list.

Add column — Display submenus and select a source, **From Database table** or **From Archive File**, for a column selection list. Use the list to add one or more column names to the **Column List**.

Note: **Add column** is available only from the blank row at the bottom of the **Column List**.

Select **From Database table** to display the **File Access Definition Table/Column Selection** dialog listing columns in the database table. For more information, see **Selecting Columns from a Table**.

Select **From table in Archive File** to display the **Open** dialog, from which to choose an Archive File before displaying the **File Access Definition Table/Column Selection** dialog. For more information, see **Selecting Columns from a Table in an Archive File**.

Note: Access permissions in the associated ACL determine the options and actions that are available to you. For example, the **Remove** shortcut menu options are not available to roles limited to read access.

Column Access Control

Use the **Column Access Control** list to define access permissions for the entry in the **Column List**. You can assign access permissions to roles in the ACD and a default for all user accounts and roles for which access permissions are not assigned explicitly. If the **AC Type** for an entry in the **Column List** is None, **Column Access Control** list is blank and cannot be edited.

Role **(Default)** and names of roles for which the File Access Definition explicitly controls access. Role names not included in the Access Control Domain that serves as the basis for the FAD are italicized and settings for them have no effect.

Notes:

- If a user is included in multiple roles in the list, the most restrictive permission applies.
- Unless the **AC Type** for the Column List entry is None, the **Column Access Control** list includes a **(Default)** setting. This default cannot be deleted and applies to users for which no explicit permissions are granted.

Type the name, or use the drop-down list to select the name of a role defined in the ACD. You can also edit a role name. To remove a role name, use the **Remove** commands in the shortcut menu.

Access The type of access permissions for the role. Select one of the following:

Allow The role is allowed access to the column.

Deny The role is denied access to the column.

You must select either **Allow** or **Deny** for **(Default)**. Roles for which both **Allow** and **Deny** are blank assume the permission selected for **(Default)**.

Note: If a role is denied access to any file attachment pseudocolumn in an Archive File, the role cannot use the Archive File in a Delete, Restore, Update, or Insert Process.

Shortcut Menu Commands

Right-click the **Column Access Control** list to display the following shortcut menu commands:

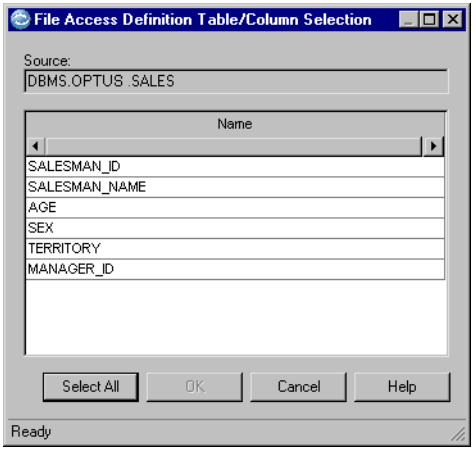
Remove	Remove the selected role from the list. (This command is not available for **(Default)**.)
Remove All	Remove all roles, except **(Default)**, from the list.
Allow all non-default	Allow access for all listed roles, except **(Default)**.
Deny all non-default	Deny access for all listed roles, except **(Default)**.

Selecting Columns from a Table

Use the **File Access Definition Table/Column Selection** dialog to select and add one or more names of columns from the table specified in the **Table Access Control** dialog to the **Column List**. **Source** displays the fully qualified table name.

To open this dialog, right-click the blank row at the bottom of the **Column List** and do one of the following:

- Select **Add column** from the shortcut menu and then select **From Database table** from the submenu.
- Select **Add column** from the shortcut menu and then select **From table in Archive File** from the submenu to first specify an Archive File containing the table.



Click a column name to select it. To select multiple columns, hold the **Ctrl** or **Shift** key while clicking the column names. To select all columns in the table, click **Select All**. Click **OK** to add the names of selected columns to the **Column List** and re-display the **Table Access Control** dialog.

Selecting Columns from a Table in an Archive File

When you select **Add table** from the **Column List** shortcut menu, and select **From table in an Archive File** from the submenu, the **Open** dialog is displayed to allow you to select an Archive File.

In the **Open** dialog, select the server on which the file resides and click **Refresh**. Use **Look In** to select the directory or path containing the file, and double-click a listed file **Name** or enter the **File Name** and click **Open**. The names of columns in the selected table are listed in the **File Access Definition Table/Column Selection** dialog. **Source** indicates the fully qualified name of the table.

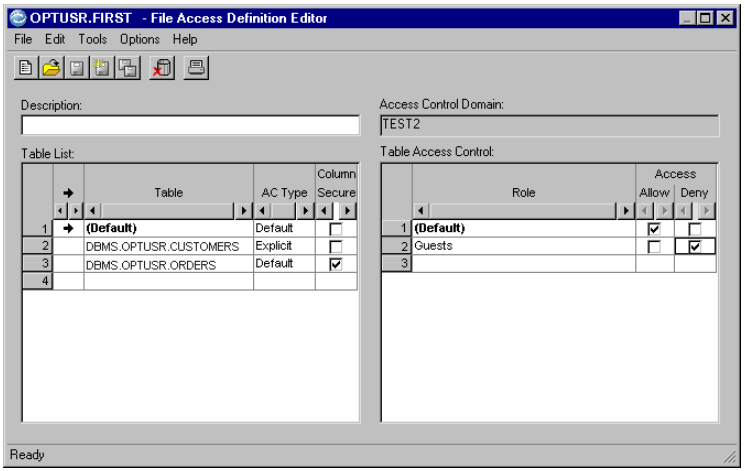
Note: The selected Archive File must contain a table with a fully qualified name that matches the name in **Table** on the **Table Access Control** dialog.

D.3.3 File Access Definition Example

The following example File Access Definition includes three types of access: a default, a restricted table (CUSTOMERS), and a restricted column (ORDERS.ORDER_ID). The roles specified in the example are part of the PSTUSER **Access Control Domain**. The ACD validates the roles and associates them with users in your network.

Default Access

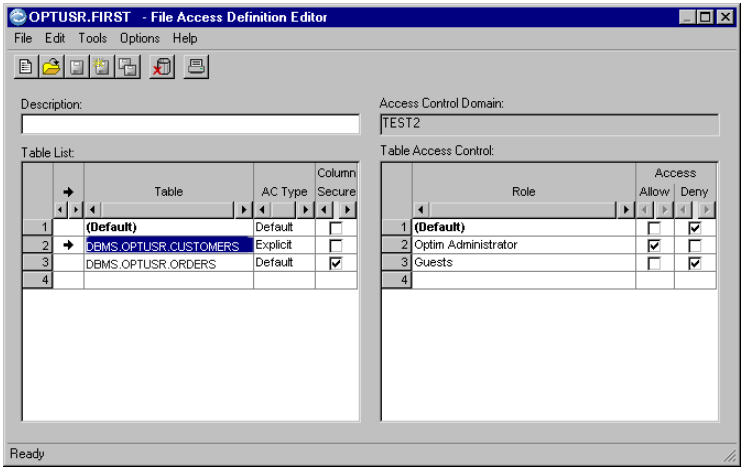
For the first entry on the **Table List**, **(Default)**, all roles and users, except the Guest role, are allowed to access tables in the Archive File that are not listed in **Table List**.



- In the **Table List**, the **(Default)** setting, for tables not listed, uses the Default **AC Type**. The Default **AC Type** assigns access permissions to the **(Default)** setting and any other tables that use Default.
- In the **Table Access Control** list, the **(Default)** setting, for users not included in the ACD and roles not specified in the list, is assigned Allow access. The Guest role is assigned Deny access.

Restricted Table

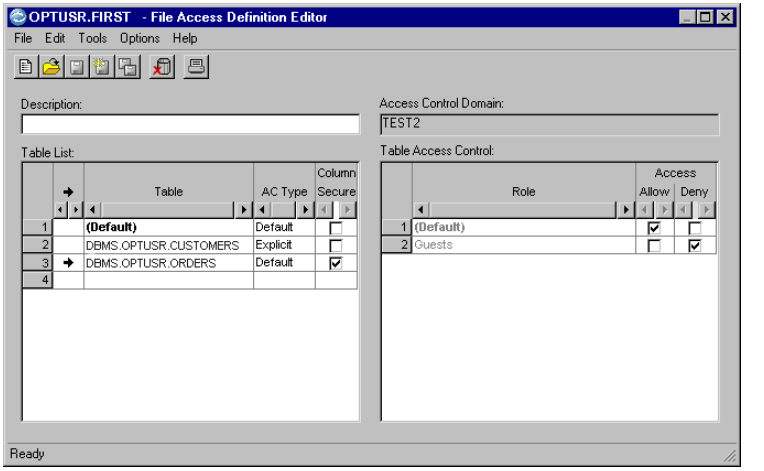
For the CUSTOMERS table, only the ***Optim*** Administrator role is allowed access. All other users and roles are denied access.



- In the **Table List**, the **AC Type** for CUSTOMERS is Explicit. The access permissions apply to this table only.
- In the **Table Access Control** list, the Optim Administrator role is assigned Allow access, and the **(Default)** setting, representing users not included in the ACD and roles not specified in the list, is assigned Deny access.

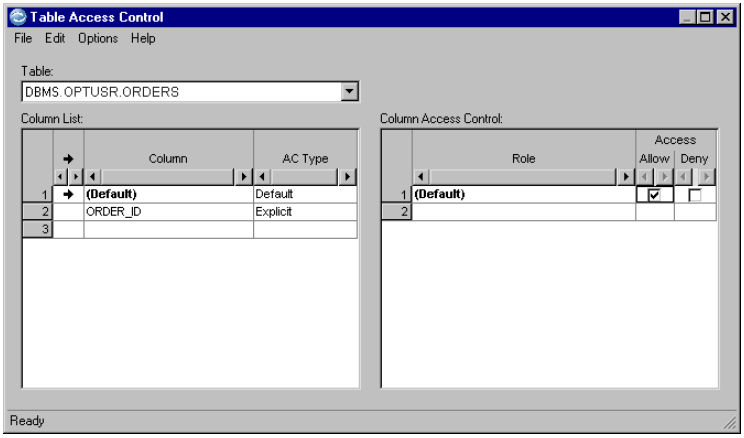
Restricted Column

For the ORDERS table, all users, except the Guest role, are allowed access, but one or more columns have separate access permissions, as indicated by **Column Secured** setting.

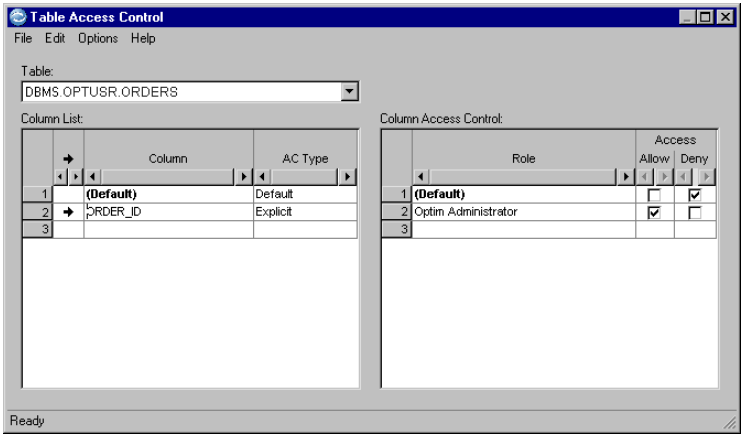


- The **AC Type** for the ORDERS table is Default, which for this File Access Definition, allows access to all users and roles, except the Guest role.
- The **Column Secured** setting indicates that one or more columns in the table have defined access permissions. To view a list of the secured columns, right-click the ORDERS row and select **List Columns**.

As shown by the **Table Access Control** dialog, the Default **AC Type** grants all users Allow access. All users that can access the table are allowed to access columns not specified in the **Column List**.



However, only the Optim Administrator role can access the ORDER_ID column. All other users and roles are denied access.



- In the **Column List**, the **AC Type** for ORDER_ID is Explicit. The access permissions apply to this column only.
- In the **Column Access Control** list, the Optim Administrator role is assigned Allow access, and the **(Default)** setting, representing users not included in the ACD and roles not specified in the list, is assigned Deny access.

D.4 Exporting Security Definitions

Use the Export Security Definitions Utility to export security definitions (ACDs, ACLs, and FADs) from one ***Optim*** Directory to another. The Export Security Definitions Utility eliminates the need to recreate security definitions manually and allows you to use the same definitions with the imported objects they secure.

To export security definitions:

1. In the main window, select **Export...** from the **Security** submenu on the **Options** menu to open the **Export Security Definitions** dialog.
2. In **Definitions**, select the security definitions to export.
3. Enter a **Secured Output File** name.
4. Type a Secured Output File **Password**.
5. Re-type the password in **Verify Password**.
6. Choose **Run** from the **File** menu.
7. Monitor progress in the **Export Progress** pane.
8. When Security Definition Export processing is finished, choose **Show Process Log** from the **Tools** menu to review or print the **Security Export Process Log**.

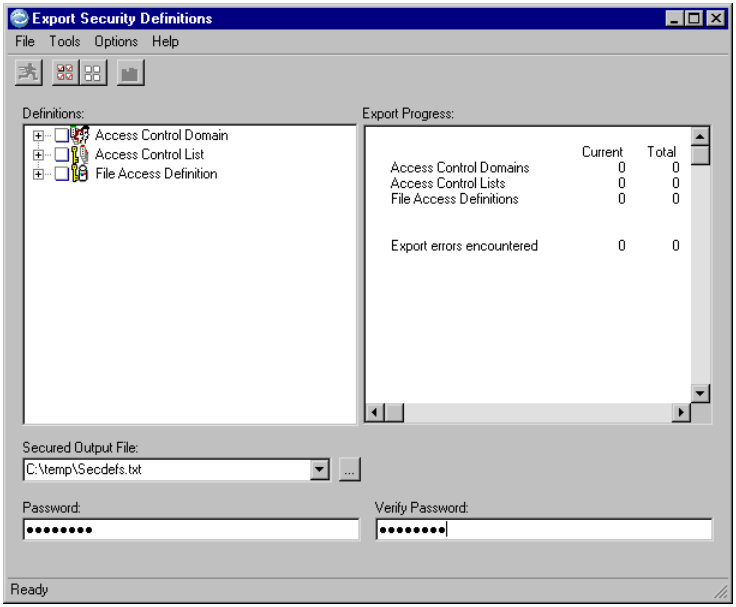
Export Security Definitions Dialog

When you open the **Export Security Definitions** dialog, the tree hierarchy on the **Definitions** pane is populated with the security definitions in the ***Optim*** Directory to which you have read access.

Notes:

- ACLs that secure ACDs and FADs are not listed but will be exported with these definitions.

- The **(Default)** ACD is not listed and cannot be exported.



You can select the check box for a security definition type in order to export all definitions of that type or expand the list and select the definitions to be exported. **Tools** menu commands allow you to select or de-select all definitions.

Secured Output File The name of the Secured Output File. The Secured Output File is a text file and is given a **.txt** extension automatically, but other extensions may be used. The Secured Output File is used as the Secured Input File for Security Definition Import processing.

Password Password for securing the Secured Output File. This password must be entered when using the file with the Security Definition Import Process.

Verify Password Re-enter the **Password** for verification.

Tools Menu The following commands are available from the **Tools** menu.

Select All Definitions Select check boxes for all listed security definitions. This command is especially useful when you want to export all or most definitions.

Deselect All Definitions	Clear the check boxes for all listed security definitions, including shaded and/or selected check boxes.
Show Process Log	Display the **Security Export Process Log** generated by the last execution of Security Definition Export.

Run Export

To export security definitions, choose **Run** from the **File** menu.

Notes: The **Run** command will not be available until you have specified security definitions for export, a Secured Output File, and a password.

During Security Definition Export processing, the **Export Progress** pane displays the number of security definitions of each type that are exported and the number of errors encountered.

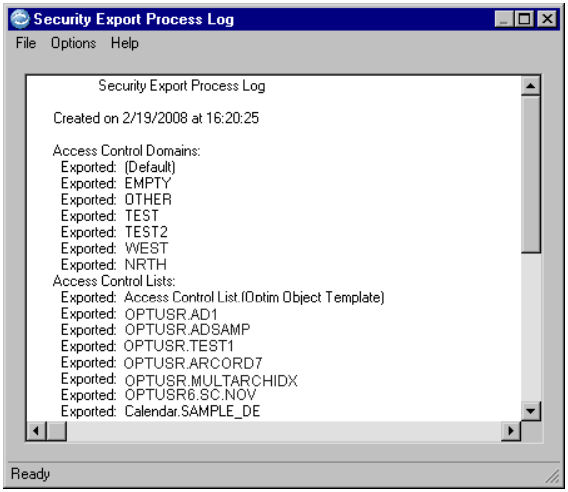
The status bar displays information about the current security definition that is processed. When Security Definition Export processing is finished, the status bar displays the message "Ready."

Export Errors

If errors occur during Security Definition Export processing (for example, a dropped definition is selected for export), an error message is displayed. Definitions for which processing errors occur are also represented visually by a red "X". Errors and diagnostic information are written to the **Security Export Process Log**.

Security Export Process Log

When the Security Definition Export is complete, select **Show Process Log** from the **Tools** menu to display the **Security Export Process Log**.



This log displays the following details:

Creation Date	Date and time the **Security Export Process Log** was created.
List of errors	Explanatory text for each error if errors were encountered.
List of exported objects	Names of the exported security definitions, grouped by object type.

Print

Print the log by choosing **Print** from the **File** menu. Each execution of Security Definition Export clears the log file before information for the current execution is written. Previous log information is not retained.

D.5 Import Security Definitions

The Import Security Definitions Utility copies security definitions from a Secured Input File to the current ***Optim*** Directory. (A Secured Output File generated by Security Definition Export is used as the Secured Input File.)

To import security definitions:

1. In the main window, select **Import...** from the **Security** submenu on the **Options** menu to open the **Import Security Definitions** dialog.
2. Specify a **Secured Input File** name. The **Import Security Definition Validation** pop-up is displayed.
3. Type the **Password** for the Secured Input File and click **OK**.
4. Select options on the **Process**, **Owners**, and **Objects** tabs.
5. Choose **Run** from the **File** menu.
6. Monitor progress in **Import Progress**.
7. Choose **Show Process Log** from the **Tools** menu to review or print the **Import Process Log**.

D.5.1 Import Dialog

The **Import Security Definitions** dialog has three tabs. Each tab and menu command available on the dialog serves a unique purpose.

Process Identify the Secured Input File, select security definitions you want to import, and provide parameters for Security Definition Import processing.

Owners Change the owner of ACLs you want to import.

Objects Designate names for the imported security definitions.

File Menu

Set as Default	Save your entries on the **Import Security Definitions** dialog as the default specifications. The settings for the following options on the **Process** tab are saved: • Allow ACL for non-existent ***Optim*** Objects • Overwrite existing definitions • Continue import if error(s)

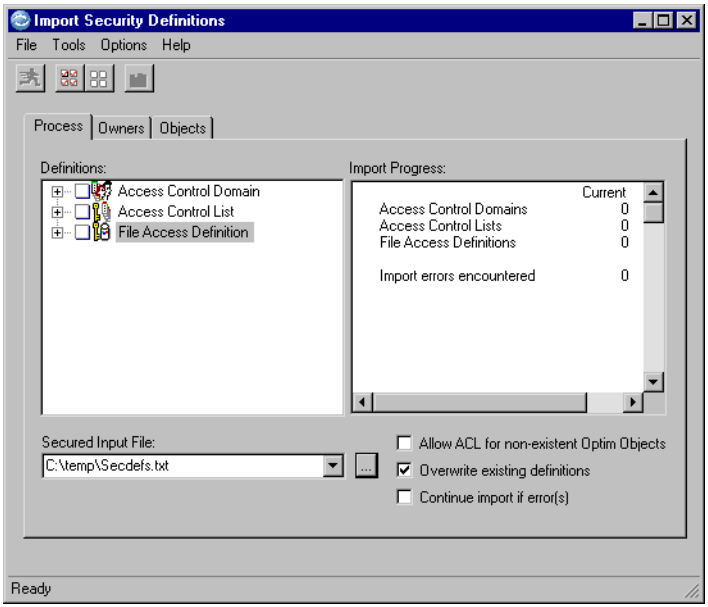
Tools Menu

The following commands are available from the **Tools** menu.

Select All Definitions	Select check boxes for all listed security definitions. This command is especially useful when you want to import all or most security definitions.
Deselect All Definitions	Clear the check boxes for all listed security definitions, including shaded and/or selected check boxes.
Show Process Log	Display the **Security Import Process Log** generated by the last execution of Security Definition Import.

Process Tab

Use the **Process** tab to identify the Secured Input File, select security definitions for import, and provide parameters for Security Definition Import processing. The tab is populated with defaults you have specified.



Definitions

The Import Security Definitions Utility populates the list of security definitions by:

- Identifying the security definitions in the Secured Input File. If there are no definitions of a specific type (e.g., no FADs), the check box for the definition type is shaded. Otherwise, you can expand the list of definitions of the type by clicking the plus (+) sign.
- Scanning the ***Optim*** Directory and identifying the security definitions in the Secured Input File that exist in the Directory. The check box to the left of each listed definition is selected or not according to the **Overwrite existing definitions** setting.
  - If **Overwrite existing definitions** is not selected, the check boxes to the left of definitions that exist in the current ***Optim*** Directory are shaded and selected and are unavailable for Import.

– If **Overwrite existing definitions** is selected, all check boxes to the left of each security definition are cleared and any definition can be selected. If a selected definition exists in the ***Optim*** Directory, Security Definition Import overwrites it.

Note: At least one available security definition must be selected to run the Security Definition Import Process.

Import Progress

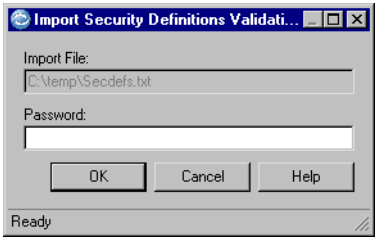
Statistics detail the current and total number of security definitions imported (by definition type) and the current and total number of errors encountered (the "total" numbers are the composite counts for all Security Definition Import Processes performed in the session). This display is updated during processing. The status bar displays information about the definition being processed.

Secured Input File

Specify a Secured Input File generated by the Security Definition Export Process (for details about creating this file, refer to **D.4 Exporting Security Definitions**).

- To select from a list of recent file names, click the down arrow or use the browse button. You may also copy a name into the box or type a name directly.
- If you do not provide a fully qualified path, the path from Personal Options is used.
- If no path is given in Personal Options, the current drive and directory are assumed.

After a Secured Input File is specified, the **Import Security Definitions Validation** pop-up is displayed. Type the **Password** and click **OK** to access the file.



Allow ACL for non-existent Optim Objects

Indicate if ACLs can be imported without having corresponding secured objects in the ***Optim*** Directory. Importing ACLs before corresponding secured objects allows the objects to be secured when they are imported.

If secured objects are imported before the corresponding ACLs, the objects are unsecured until the ACLs are imported.

If a corresponding secured object is never imported, the ***Optim*** Directory will contain ACLs that do not secure an object (orphan ACLs). If an object is created with a name that matches an orphan ACL, that ACL will be associated with the object.

- To import ACLs for secured objects that do not exist in the ***Optim*** Directory, select this check box.
- To prevent importing ACLs for secured objects that do not exist in the ***Optim*** Directory, clear the check box.

Overwrite existing definitions

Indicate the action taken when the name of an imported security definition matches a definition already in the current ***Optim*** Directory:

- To overwrite existing definitions in the Directory and select any or all security definitions for import, select the check box.
- To prevent overwriting security definitions, clear the check box. Duplicate definitions, indicated by check boxes that are shaded and selected, are not imported.

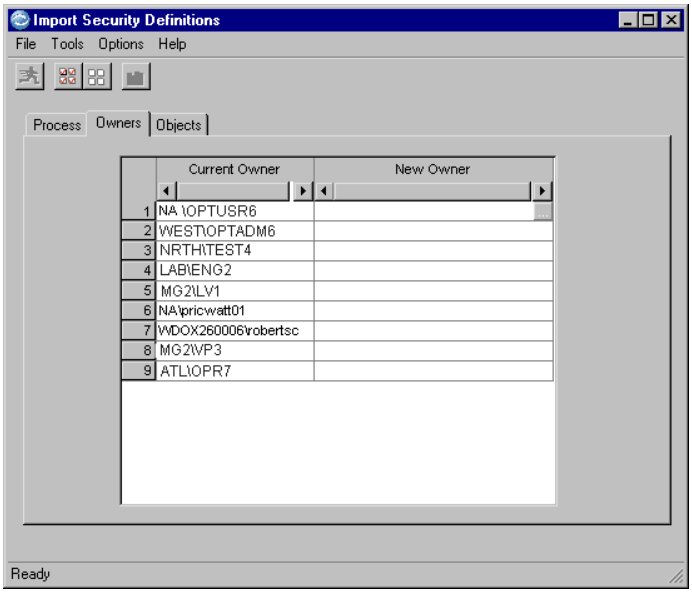
Continue import if error(s)

Indicate processing if an error occurs. Errors are written to the **Security Import Process Log** and displayed on the message bar.

- To continue processing if an error occurs, select the check box.
- To halt processing if an error occurs, clear the check box.

Owners Tab

Use the **Owners** tab to review or change the owner name of ACLs you want to import.



Current Owner A read-only list of the owners of each ACL in the Secured Input File.

New Owner Specify a new owner name for an ACL in the Secured Input File. Use the browse button to open the **Security Users** dialog and select an owner (see **Security Users**).

Shortcut Menu Commands Right-click to select from the following shortcut menu commands:

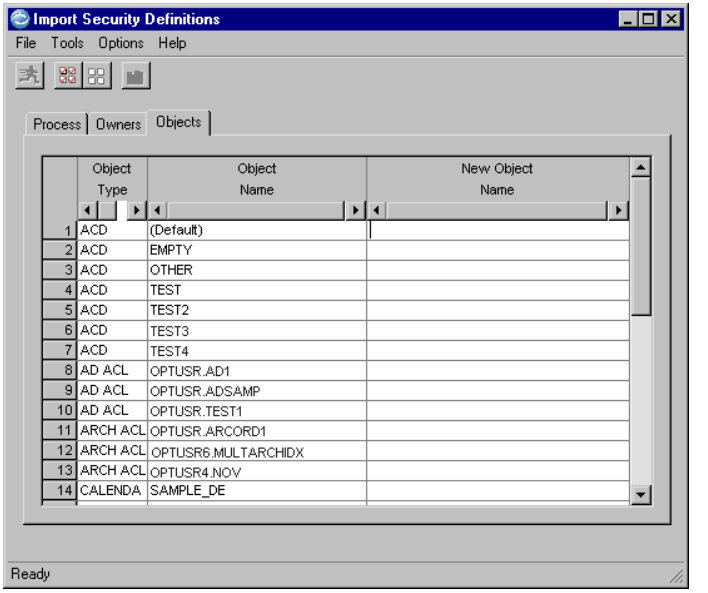
Copy Name Copies the Current Owner name to the New Owner column for the ACL. Available in the Current Owner column only.

Populate

- **Clear** Copies the Current Owner name to the New Owner column for all ACLs.
- **Add** Copies the Current Owner name to the New Owner column for ACLs without a New Owner name.
- **Empty** Empties names from the New Owner column for all ACLs.

Objects Tab

Use the **Objects** tab to review or change the names of security definitions you want to import.



Object Type

Identifies the security definition as an ACD, ACL, or FAD. For ACLs, the following abbreviations identify the secured object types:

AD	Access Definition
ARCH	Archive Request
CALENDAR	Calendar
CM	Column Map
CMPROC	Column Map Procedure
COMP	Compare Request
CONV	Convert Request
CURRENCY	Currency Table
DBALIAS	DB Alias

DEL	Delete Request
ED	Edit Definition
EXTR	Extract Request
LOAD	Load Request
PK	Primary Key
REL	Relationship
REPT	Report Request
REST	Restore Request
STORPROF	Storage Profile
TM	Table Map
UPIN	Update or Update/Insert Request

Object Name The names of the security definitions available for importing.

New Object Name Specify a new name for the security definition. The name must comply with the naming conventions for the security definition.

Shortcut Menu Commands Right-click to select from the following shortcut menu commands:

Copy Name Copies the Object Name to the New Object Name column for the security definition. Available in the Object Name column only.

Populate

- **Clear** Copies the Object Name to the New Object Name column for all security definitions.
- **Add** Copies the Object Name to the New Object Name column for security definitions without a New Object Name.
- **Empty** Empties names from the New Object Name column for all security definitions.

Run Import

To import security definitions, choose **Run** from the **File** menu.

Note: The **Run** command will not be available until you select at least one available security definition.

During Security Definition Import processing, the **Import Progress** pane displays the number of security definitions of each type that are imported and the number of errors encountered.

The status bar displays information about the current security definition that is processed. When Security Definition Import processing is finished, the status bar displays the message "Ready."

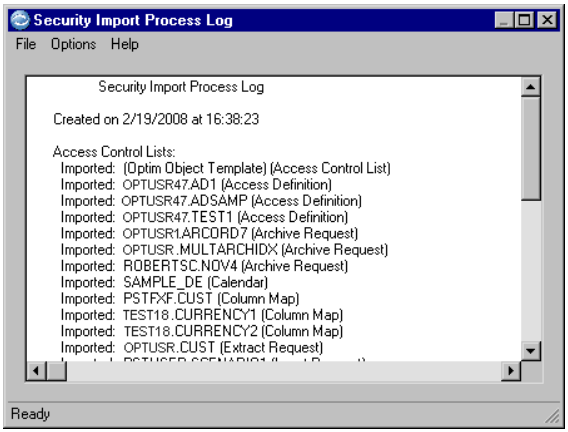
Import Errors

If the Import Security Definitions Utility encounters errors, processing continues according to the specification for the **Continue import if error(s)** option. Errors are displayed on the message bar and represented visually by a red "X" beside each security definition in error. Errors are written to the **Security Import Process Log** after Import Processing is finished. You can review and print the **Security Import Process Log** for diagnostic information about errors.

If some objects fail to be imported due to errors, check the specifications, and try Export and Import again.

Import Process Log

When Security Definition Import Processing finishes, select **Show Process Log** from the **Tools** menu to display the **Security Import Process Log**.



Creation Date	Date and time the **Security Import Process Log** was created.
List of errors	Explanatory text for each error if errors were encountered.
List of imported objects	Names of the imported security definitions, listed by object type and name.

Print

Print the log by choosing **Print** from the **File** menu. Each execution of the Security Definition Import clears the log before information for the current execution is written. Previous log information is not retained.

Appendix E. Security Reports

Using the Report Process, you can create a report on the permissions for Functional or Object Security privileges assigned to user and group accounts in your network.

You can also create a report on the contents of an Archive or Compare File or list Archive Directory entries that meet criteria you supply (for more information about these reports, see the ***Archive*** or ***Compare*** **User Manual**).

Security Reports

Security permissions allow or deny roles, which consist of user and group accounts, privileges such as the ability to open a dialog, run a process, or modify a specific object. Security Reports allow you to see which users and groups have permissions for these privileges and the roles to which the permissions apply. For more information about security privileges, see **Appendix D. Optim Security**.

Depending on your specifications, you can create a report that will:

- List the Functional Security permissions assigned to specified users and groups.
- List all Functional Security permissions for selected privileges.
- List the Object Security permissions for specified users and groups that apply to specified objects and the ACL that secures each object.

Report Process

The Report Process runs on the workstation (not on the ***Optim Server***). Specifications for a Report Process are stored as a Report Request. Use the Report Request to provide the report criteria and processing options. The **Report Process Report** dialog displays the report.

Run or Schedule

You can process a Report Request immediately (by selecting **Run** from the **File** menu) or you can schedule the request for processing at a later time (by selecting **Schedule** from the **File** menu).

Naming Conventions

A fully qualified Report Request name is in the form *identifier.name*, where:

identifier Identifier assigned to the Report Request name (1 to 8 characters).

name Base name assigned to the Report Request (1 to 12 characters).

A logical set of naming conventions can identify the use for each Report Request and be used to organize them for easy access.

Chapter Contents

This chapter explains how to create, maintain and process a Report Request, including how to:

- Select the type of Security Report.
- Provide criteria and values for the report.
- Run, save, and schedule a Report Request.

E.1 Open the Report Request Editor

Use the **Report Request Editor** to create or edit requests for Security Reports. You can store these requests in the ***Optim*** Directory. There are different ways to open the editor, depending on whether you want to create a new Report Request or edit an existing a Report Request.

E.1.1 Create a New Report Request

You can create a Report Request from the main window or from the **Report Request Editor**.

From the Main Window

To create a Report Request:

1. In the main window, select **New** from the **File** menu.
2. Select **Report** from the **Actions** submenu to open the **Report Request Editor**.
3. On the **General** tab, select **Security** in the **Report Type** list, and provide an optional title for the report.
4. On the **Security Criteria** tab, enter criteria for a Security Report.
5. In the **Report Request Editor**, select **Save** from the **File** menu to open the **Save a Report Request** dialog.
6. In the **Pattern** box, type a unique name for the new Report Request and click **Save**.

From the Report Request Editor

To create a Report Request from the Editor:

- To create a new Report Request, select **New** from the **File** menu in the **Report Request Editor**.
- To create a new Report Request modeled on an existing one, open the desired Report Request and select **Save As** from the **File** menu.
- To create and store a copy of the active Report Request and continue editing, select **Save Copy As** from the **File** menu.

These steps are the minimum required to create a Report Request. After you create a request, you can run the process immediately, or save the request and schedule it. Because the options to create a Report Request and to modify a Report Request are similar, refer to **E.2 Using the Editor** for complete details.

E.1.2 Select a Report Request to Edit

You can select a Report Request for editing from the main window or from the **Report Request Editor**.

From the Main Window

To Select a Report Request to Edit:

1. In the main window, select **Open** from the **File** menu to display the **Open** (object selection) dialog.
2. Double-click to select **Report Request** and expand the Identifier list.
3. Double-click the Report Request Identifier to display a list of Report Requests.
4. ***Optional*** – Specify a **Pattern** to limit the list based on your criteria and click **Refresh**.
5. Double-click the grid row for the desired Report Request to open the **Report Request Editor**.

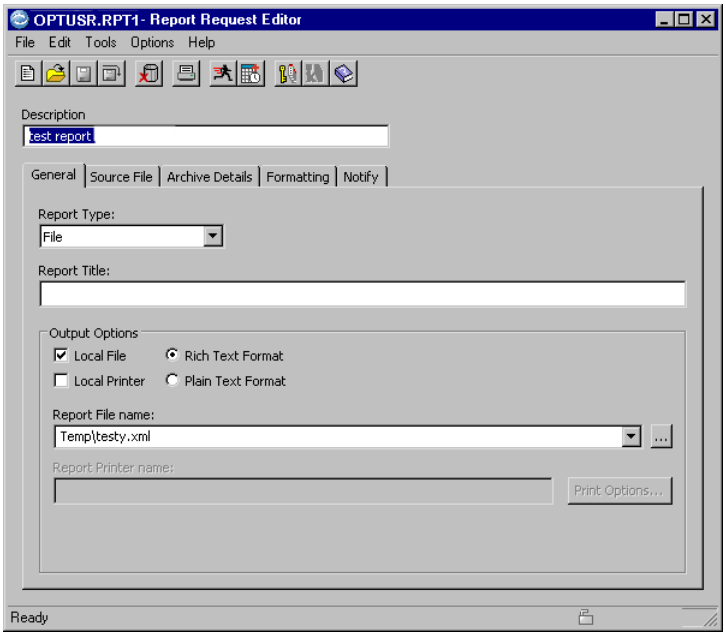
To select the last Report Request you edited:

- In the main window, select **Report Request** from the **Actions** menu to open the **Report Request Editor** and the last edited Report Request.

When you select the **Open** command from the **File** menu in the main window or an editor, the **Open** dialog is displayed. For more information about this dialog, see the **Common Elements Manual, Chapter 2. Main Window, Menus, and Dialogs**.

E.2 Using the Editor

In the **Report Request Editor** you can create, modify, or delete Report Requests. You can also save Report Requests to the ***Optim*** Directory.



Description Text to describe the purpose of the Report Request (up to 40 characters).

Tabs Use the **Report Request Editor** tabs to provide parameters and select options to define Report Requests. Each tab in the editor serves a unique purpose.

General Parameters required by the Report Process, including the type of report (i.e., Security), the report title, output options, report file name, and printer specifications, as applicable. Each time you open the editor, the **General** tab is shown first.

Security Criteria Parameters needed to create a report on permissions for Functional or Object Security privileges. The **Security Criteria** tab is available when **Report Type** on the **General** tab is set to **Security**.

Archive Criteria	Parameters needed to select entries in the Archive Directory for the report. The **Archive Criteria** tab is available when **Report Type** on the **General** tab is set to **Archive Directory**. For more information, see the ***Archive* User Manual, 7.2.2 Archive Criteria Tab**.
Source File	Parameters needed to select an Archive or Compare File for the report. The **Source File** tab is available when **Report Type** on the **General** tab is set to **File**. For more information, see the ***Archive* User Manual, 7.2.3 Source File Tab** or ***Compare* User Manual, 6.2.2 Source File Tab**.
Archive Details	Layout and row display options for the report. The **Archive Details** tab is available when **Report Type** on the **General** tab is set to **File** and the Source File is an Archive File. For more information, see the ***Archive* User Manual, 7.2.4 Archive Details**.
Compare Details	Layout and row display options for the report. The **Compare Details** tab is available when **Report Type** on the **General** tab is set to **File** and the Source File is a Compare File. For more information, see the ***Compare* User Manual, 6.2.3 Compare Details Tab**.
Formatting	Limits, spacing, and table heading options for the report. The defaults for formatting options are set in Product Options. The **Formatting** tab is available only when **Report Type** on the **General** tab is set to **File**.
Notify	Options for automatic email notification of the success or failure of the process.

Tools Menu Commands

In addition to the standard commands on the **File**, **Edit**, and **Tools** menus, you can select the following commands from the **Tools** menu:

Convert to Local	Convert a named Report Request to a local Report Request. A local Report Request is saved with the Archive Request. Available only when the **Report Type** on the **General** tab is set to File.
Edit Joins	Open the **Edit Joins** dialog to select joined tables in the report. Available when **Show Joins** is selected on the **Archive Details** tab and the **Report Type** on the **General** tab is set to File.

E.2.1 General Tab

Use the **General** tab to select the report type.

Report Type

Select the type of report:

File	Report on data in a Source Archive or Compare File. For more information, see the ***Archive* User Manual**, **7.2.1 General Tab** or ***Compare* User Manual, 6.2.1 General Tab**.
Archive Directory	Report on selected Archive Directory entries and the properties of associated Archive Files. For more information, see the ***Archive* User Manual, 7.2.2 Archive Criteria Tab**.
Security	Report on Functional or Object Security permissions.

Report Title

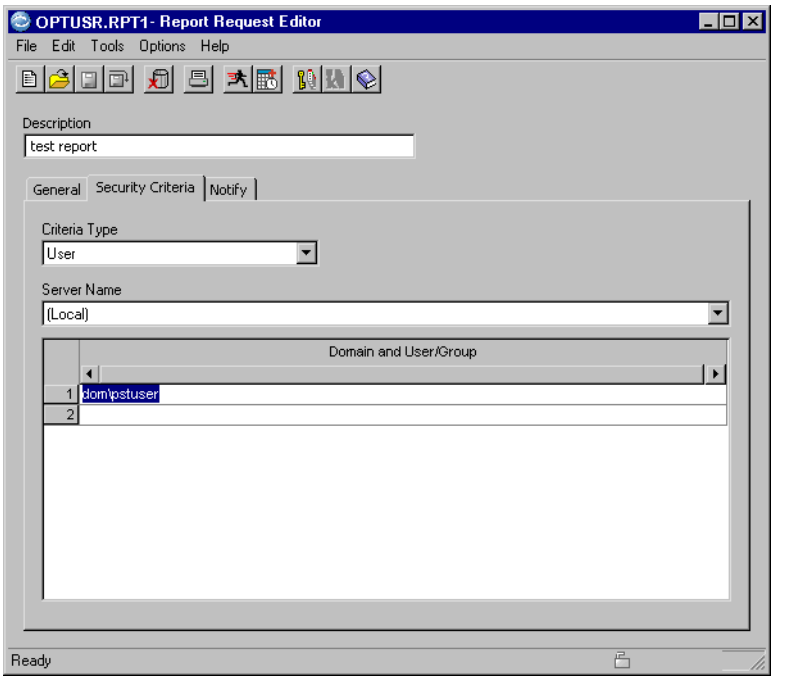
The **Report Title** is not available for Security Reports.

Output Options

The **Output Options** are not available for Security Reports. You can save and print a report from the **Report Process Report** dialog.

E.2.2 Security Criteria

Use the **Security Criteria** tab to define criteria for reports on permissions for Functional or Object Security privileges. Permissions apply to users and groups defined in roles in an Access Control Domain (ACD). Functional Security reporting lists permissions defined in the **(Default)** ACD. Object Security reporting lists permissions defined in the ACD associated with the Access Control List (ACL) that secures a specified object. For more information about ACDs, ACLs, and security privileges, see **Appendix D. Optim Security**.



Criteria Type

Select a Security Report type:

User Lists Functional Security permissions for specified users and groups.

Function Lists all Functional Security permissions for selected privileges.

Object Lists Object Security permissions for specified users and groups that apply to specified objects and the ACL that secures each object.

Server Name

For User and Object Security Reports. Select the name of an ***Optim Server*** or the (Local) workstation that the Report Process will use to verify user and group names. The machine must be part of the domain or node where the accounts of the user and group names in the report are defined.

User Report

The User Security Report lists Functional Security permissions for specified users and groups. The report lists each privilege class and permissions for the associated privileges as well as the role to which a permission applies. If a user is a member of a group for which Functional Security is defined, the group is included. You can use wildcards for criteria.

Domain and User/ Group

Enter user or group names in the format *domain\name*, or "everyone" to include all group and user names in all domains and nodes. Enter one name per line.

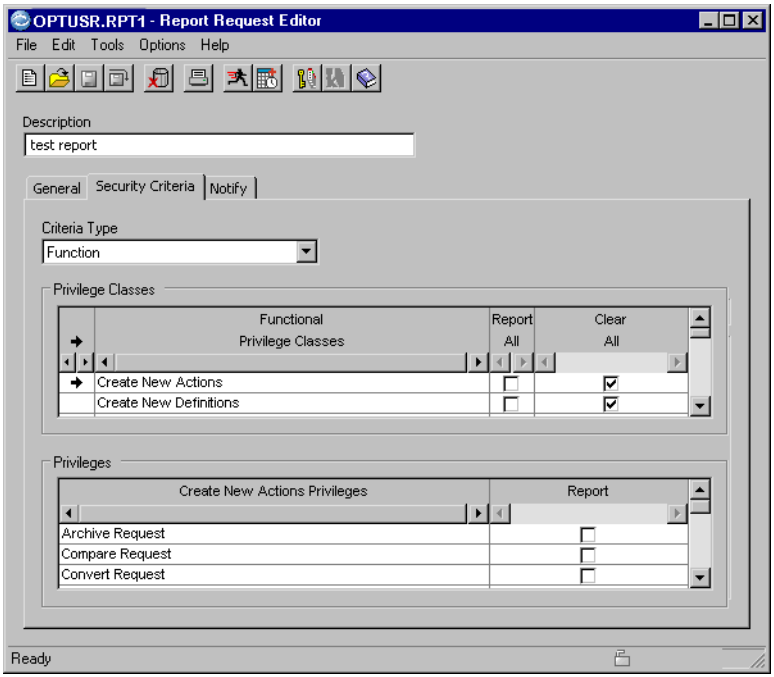
You can use percent (%) as a wild card character, but the pattern must use the *domain\name* format. For example, *dom\n%* or *%\%*.

Function Report

The Function Security Report lists Functional Security permissions assigned to each user and group for selected privileges as well as the role to which they apply.

The tab is divided into two grids, one for privilege classes and one for privileges that are included in the selected privilege class. For a

description of Functional Security privilege classes and privileges, see **Functional Privileges Tab** on page 458.



Privilege Classes

Use the Privilege Classes grid to display associated privileges in the Privileges grid. You can also use the Privilege Classes grid to select all associated privileges for reporting or clear all associated privileges selected for reporting.

To select a row in the Privilege Classes grid, click a row indicator cell or either a **Report All** or **Clear All** cell. The grid arrow, ➔, indicates the class of privileges displayed.

To include all associated privileges in the report, select **Report All**. To remove all selections in the Privileges grid, select **Clear All**.

Privileges

Use the Privileges grid to select privileges to include in the report. To include a privilege, select **Report**.

Shortcut Menu Commands

Right-click the Privileges Classes grid to display the following shortcut menu commands:

Report All Classes Select **Report All** for all privilege classes.

Clear All Classes Select **Clear All** for all privilege classes.

Right-click the Privileges grid to display the following shortcut menu commands:

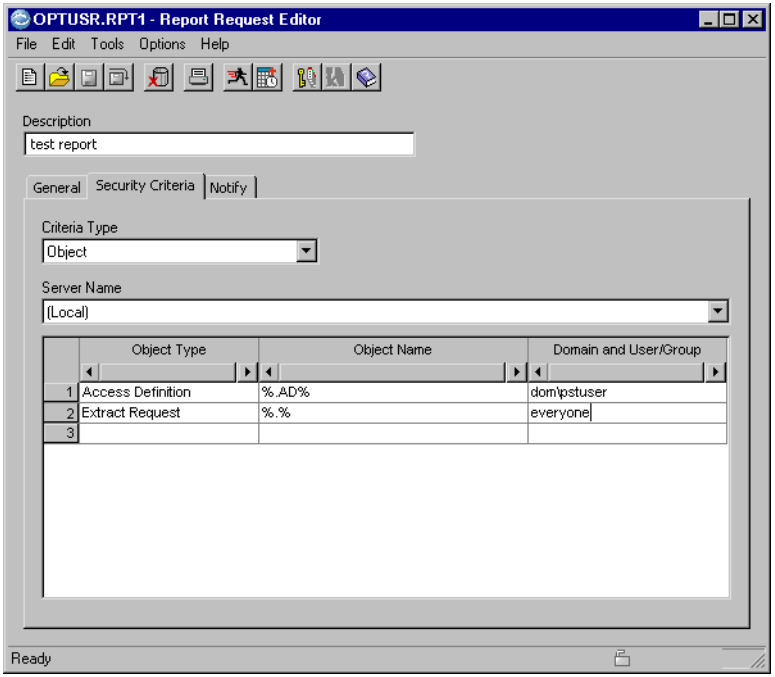
Report All Select **Report** for all privileges.

Clear All Clear **Report** for all privileges.

Object Report

The Object Security Report lists Object Security permissions assigned to specified users or groups for specified ***Optim*** objects and the ACL that secures each object. You can use wildcards for criteria. The report is sorted alphabetically by object type.

Note: The Object Security Report allows you to view permissions for ACLs for which you do not have read access.



Object Type Select an object type.

Object Name Enter an object name. You can use percent (%) as a wild card character, but the pattern must match the object name format. For example, if an object uses a two-part name, enter *own%.nam%*.

Domain and User/ Group Enter user or group names in the format *domain\name*, or "everyone" to include all group and user names in all domains and nodes. Enter one name per line.

You can use percent (%) as a wild card character, but the pattern must use the *domain\name* format. For example, *dom\n%* or *%\%*.

E.2.3 Notify Tab

Use the **Notify** tab to specify options and addresses for automatic email notification of the success or failure of the process. The process report generated when the process completes is automatically sent as an attachment.

E.3 Process a Report Request

A Report Request processes in several steps. There are a few differences depending on whether you schedule the process or run the Report Request immediately. The steps are described in the following paragraphs.

E.3.1 Schedule a Report Process

To schedule a Report Process to run once or repeatedly at a specified future time, save the Report Request and select Schedule from the File menu.

- Processing is initiated at the scheduled time; you do not review the Report Process as it is performed.
- If warning conditions exist, processing continues without prompting, depending on the **Stop on Error** parameter you specified on the **Steps** tab of the **Scheduling Job** dialog.
- If an error occurs during the Report Process, processing stops.

For details on scheduling, refer to the **Common Elements Manual, Chapter 14. Schedule**.

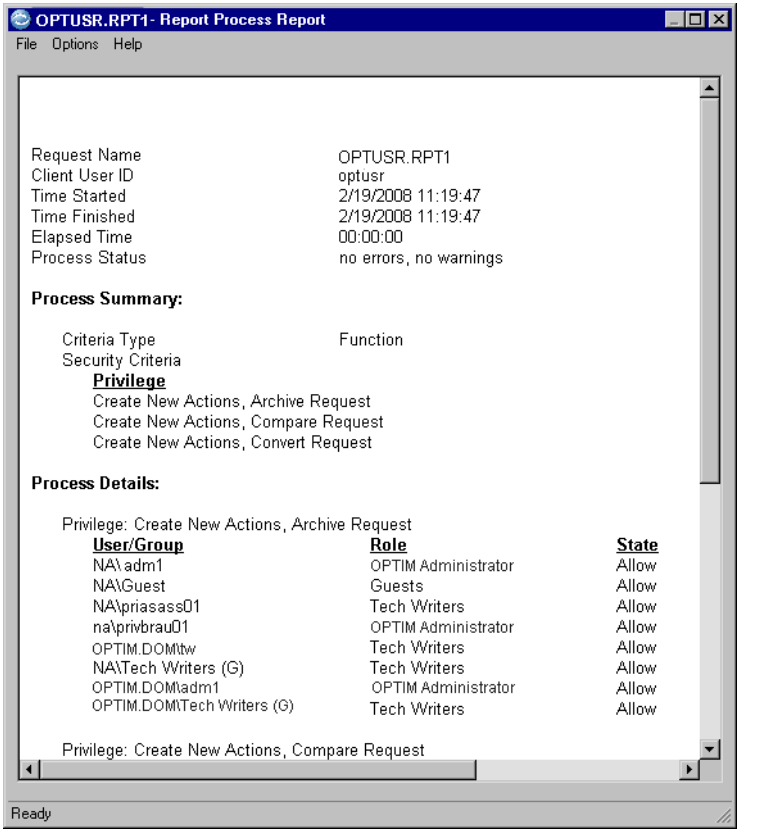
E.3.2 Run a Report Request

To process a Report Request immediately, select Run from the File menu. It is not necessary to save the Report Request before it is run.

- Before processing begins, the Report Request is verified. If errors exist, you can review the details on the message bar at the bottom of the **Report Request Editor**.
- After the Report Request has been verified, the process parameters are verified. If warnings or errors exist, you can review the details in the **Warnings** dialog and choose to continue or cancel the process.
- During processing, the **Report Request Progress** dialog displays the progress of the process and allows you to cancel the process.
- If an error occurs during the Report Process, processing stops.

E.3.3 Report Process Report

The Report Process generates a **Report Process Report** that provides general information and statistics about the Report Process. The formatting of the **Report Process Report** is determined by the **Report Type**. The following is a sample Function Security Report:



The Report Process Report displays the following information:

- Name of the Report Request (or "(Untitled)" if you did not save the request).
- User ID of the user requesting the Report Process.
- Date and time the Report Process started.
- Date and time the Report Process completed.

- The elapsed time.
- A list of any warnings or errors that occur during processing.

Process Summary

The **Criteria Type** indicates the type of Security Report: User, Functional, or Object. For User and Object Security Reports, the **Server Name** is included.

The **Security Criteria** lists the criteria entered for each Security Report type:

- For a User Security Report, each User/Group is listed.
- For a Functional Security Report, each selected privilege is listed.
- For an Object Security Report, each Object Type, Object Name, and User/Group is listed.

Process Details

User Security Reports are sorted by user/group names. Group names are indicated by a (G). The following details are included:

Privilege	Lists each privilege class above an indented list of associated privileges.
Role	The role name that includes the user or group.
State	The type of permission, Allow or Deny. "None" indicates a permission is not defined.

Functional Security Reports are sorted by privilege. The following details are included:

User/Group	The users and groups assigned permissions. Group names are indicated by a (G).
Role	The role name that includes the user or group.
State	The type of permission, Allow or Deny. "None" indicates a permission is not defined.

Object Security Reports are sorted by object type. For each object type, the report lists object names. If an object is secured, the report includes the ACD (in parentheses) associated with the ACL that secures the object, the ACL owner, and the permissions. If an object is not secured, the report will display "Not Secured" next to the object name.

Following the listed objects, a List of Used ACDs displays the ACDs listed in the report. The following details are included:

User/Group The users and groups assigned permissions. Group names are indicated by a (G).

Role The role name that includes the user or group. The "ACL Owner" is also included.

Object Access Access privileges for the object. Permissions (Allow or Deny) are listed below each privilege. "None" indicates a permission is not defined. "Owner" indicates the user is the ACL owner and allowed the privilege, overriding a permission set for another role that includes the user. "N/A" indicates the privilege does not apply to the object.

- **Read** Open or view an object.
- **Upd** Save an object.
- **Del** Delete an object.
- **Exec** Run a process request.

ACL Access Access privileges for the ACL that secures the object. Permissions (Allow or Deny) are listed below each privilege. "None" indicates a permission is not defined. "Owner" indicates the user is the ACL owner and allowed the privilege, overriding a permission set for another role that includes the user.

- **Read** View the ACL.
- **Upd** Modify the ACL.
- **Del** Delete the ACL.

Appendix F. Open Data Manager

Optim* Open Data Manager** (ODM) provides access to data in ***Optim Archive Files for programs that use the Open Data Base Connectivity (ODBC) and Java Data Base Connectivity (JDBC) Application Programming Interfaces (APIs). You can use ODM on the same Windows, Solaris, AIX, HP-UX, and Linux platforms that are supported by ***Optim***. ***Optim*** must be installed prior to installing ODM; however, ODM can be installed during the ***Optim*** installation process.

ODM is implemented using the Attunity Connect product in concert with a custom driver that provides access to Archive Files and Archive File Collections. Attunity Connect is a rich peer-to-peer networking product. A full set of Attunity manuals is included with ODM. This appendix describes how to install, configure, and use ODM to provide access to Archive Files.

Deployment Strategy

To be accessed using ODM, Archive File(s) must be registered in an ***Optim*** Directory and be accessible from the ODM Server on which the data source is defined. A primary ODM Server resides on an ***Optim Server*** machine with one or more ODM data sources for Archive Files or Archive File Collections.

If JDBC is the sole API used to access archived data, a direct connection is made to the primary ODM Server; however, you must install the Attunity Server Thin Client on each Windows workstation that will use JDBC to access archived data.

If ODBC is used to access archived data, a secondary ODM Server must be installed on each Windows workstation that will use ODBC to access archived data. A secondary server references the data source on a primary server.

You can use Attunity Studio, which is included with your ODM installation, to administer the primary and secondary servers from a single Windows machine. Attunity documentation is located in the ODM\doc subdirectory of the ***Optim*** installation directory.

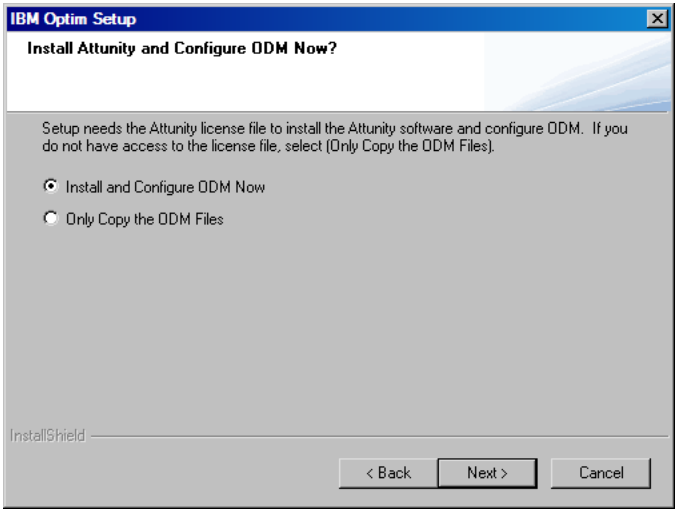
F.1 Installation

The ***Optim*** installation CD for Windows includes installation files for the ODM Server and Attunity Studio. The ***Optim*** installation CD for UNIX or Linux includes installation files for the ODM Server only.

Note: If installing Attunity Server or Attunity Studio in a Windows environment, you must remove any older versions before installation.

F.1.1 Windows Installation

To install ODM, select ODM Interface on the **Select Components** dialog of the ***Optim*** **Setup** program. You can choose to install ODM as part of the ***Optim*** installation or copy the ODM installation files to your machine for use at a later time.


IBM Optim Setup
Install Attunity and Configure ODM Now?
Setup needs the Attunity license file to install the Attunity software and configure ODM. If you do not have access to the license file, select (Only Copy the ODM Files).
Install and Configure ODM Now
Only Copy the ODM Files
InstallShield
< Back
Next >
Cancel

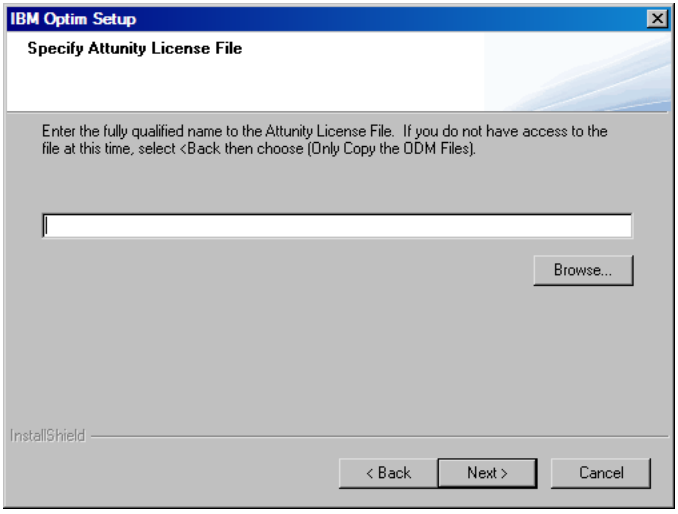
Install and Configure ODM Now Select this option to install a primary ODM Server only. You are prompted for the Attunity License file and both the ODM Server and Attunity Studio are automatically installed. The ODM Server and Attunity Studio installation files are also copied to your machine.

If both Attunity Server and Attunity Studio are installed, this option is labeled **Configure ODM Now**.

Only Copy the ODM Files Select this option to install a primary or secondary ODM Server. This option copies the ODM Server and Attunity Studio installation files to your machine. To complete the ODM installation, you must install ODM manually.

Automatic ODM Installation

After you choose **Install and Configure ODM Now** (or **Configure ODM Now**) from the **Setup** program, the **Specify Attunity License File** dialog is displayed. Enter the path to the Attunity License file, or click **Browse** to select a path.


IBM Optim Setup
Specify Attunity License File
Enter the fully qualified name to the Attunity License File. If you do not have access to the file at this time, select <Back then choose (Only Copy the ODM Files).
Browse...
InstallShield
< Back
Next >
Cancel

After you provide the license file path, click **Next** to display the **Select Program Folder** dialog (see **2.1.6 Select Program Folder** on page 44) and continue the ***Optim*** installation.

ODM is installed at the end of the ***Optim*** installation process and Command Prompt dialogs requiring no entries are displayed.

Manual ODM Installation

To install a primary ODM Server manually, you must run the ODM installation script and register the Attunity license. A primary server installation includes the ODM Server and Attunity Studio.

To install a secondary ODM Server manually, you must run the ODM Server installation file. A secondary server installation includes the ODM Server only.

To install a primary ODM Server on a Windows machine:

1. Copy the Attunity license file to a directory on your machine.
2. From a Command Prompt, access the ODM\install subdirectory of the ***Optim*** installation directory.
3. Type the following command:

   ```
   ODMINSTALL
   ```

4. When prompted to confirm the Attunity Server installation, click **OK**.
5. When prompted, type the path to the Attunity license file and click **OK**.

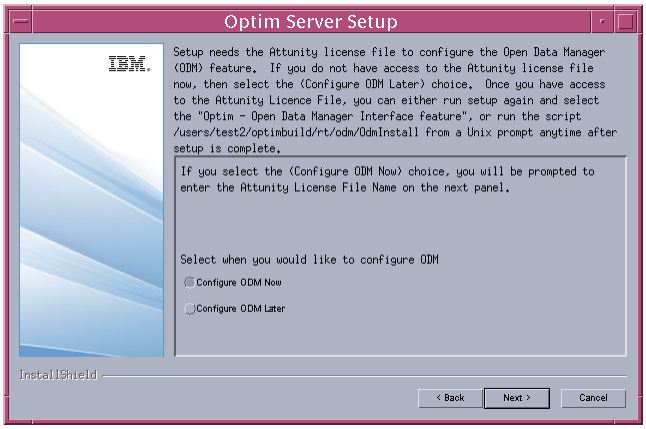
To install a secondary ODM Server on a Windows machine:

Run the ODM Server installation file, *AS4820-win32.exe*, located in the ODM\install subdirectory of the ***Optim*** installation directory.

By default, the Attunity daemon runs under the Local System account. If access to needed resources requires network credentials, the daemon logon must be changed to an appropriate network account. To change the logon account, open the **Services** dialog from the Control Panel/Administrative Tools, double-click the **Attunity Server Daemon (IRPCD)**, and specify the account on the **Log On** tab.

F.1.2 UNIX Installation

To install the ODM Server in a UNIX environment, select Open Data Manager Interface from the select components dialog of the **Server Setup** program. You can install the ODM Server as part of the **Server** installation or copy the ODM Server installation files to your machine for use at a later time.

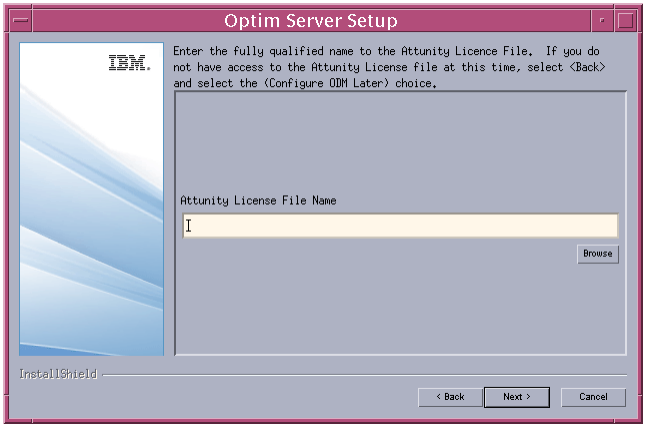

Optim Server Setup
IBM.
Setup needs the Attunity license file to configure the Open Data Manager (ODM) feature. If you do not have access to the Attunity license file now, then select the (Configure ODM Later) choice. Once you have access to the Attunity Licence File, you can either run setup again and select the "Optim - Open Data Manager Interface feature", or run the script /users/test2/optimbuild/rt/odm/OdmInstall from a Unix prompt anytime after setup is complete.
If you select the (Configure ODM Now) choice, you will be prompted to enter the Attunity License File Name on the next panel.
Select when you would like to configure ODM
Configure ODM Now
Configure ODM Later
InstallShield
< Back
Next >
Cancel

Configure ODM Now This option prompts you for the Attunity license file and automatically installs the ODM Server.

Configure ODM Later This option copies the ODM Server installation files to your machine. To complete the ODM Server installation, you must install the ODM Server and register the Attunity license manually.

Automatic ODM Server Installation

After you choose **Configure ODM Now** from the **Setup** program, the next dialog prompts you for the Attunity license. Enter the path to the Attunity License file, or click **Browse** to select a path.



After you provide the license file path, click **Next** to continue the ***Optim*** installation. When the ODM installation is complete, a terminal dialog is displayed, indicating the ODM installation was successful. Press **Enter** to close the dialog.

Manual ODM Installation

To install the ODM Server manually, you must run the ODM Server installation script and register the Attunity license file.

To install an ODM Server in UNIX

1. Run the ODM Server installation file, *OdmInstall*, located in the rt/odm/install subdirectory.
2. When prompted, type the path of the Attunity license key, *license.txt*.
3. Log off and log back on to effect changes to .profile.

Note: For users of Oracle prior to release 9.2, ODM and the Oracle Transparent Gateway use different versions of the libnvbaseshr.so library. To avoid a conflict, Oracle Transparent Gateway and ODM must be assigned to different user accounts. The shared library path environment variable (e.g., LIBPATH for AIX) for the Oracle Transparent Gateway account must reference the library in the Oracle directory before the library in the Attunity directory.

F.1.3 UNIX Administration

After ODM is installed, if it has not been done previously, you must source the RTSETENV file to set up the environment needed to run ODM. If you have added RTSETENV to your .profile or .login, source that file instead. If not, change to the directory where ***Optim*** is installed (e.g., /opt/IBM/Optim) and use:

```
$ . ./rtsetenv
```

Starting the ODM Server

Once you have set up the required environment, use the following to start the ODM Server.

```
irpcdstart
```

Stopping the ODM Server

Optim and the ODM Server share common resources. To reinstall or upgrade ***Optim***, you must shut down both ***Optim*** and the ODM Server prior to starting the installation. Use the following procedure to shut down both ***Optim*** and the ODM Server.

```
$ rtserver stop
irpcdshutdown
$ mwadm stop
```

Notes:

- Do not use ‘mwadm stop’ prior to invoking ‘irpcdshutdown,’ otherwise, you may not be able to restart ***Optim***.
- To shut down ***Optim*** only, do not invoke ‘mwadm stop.’

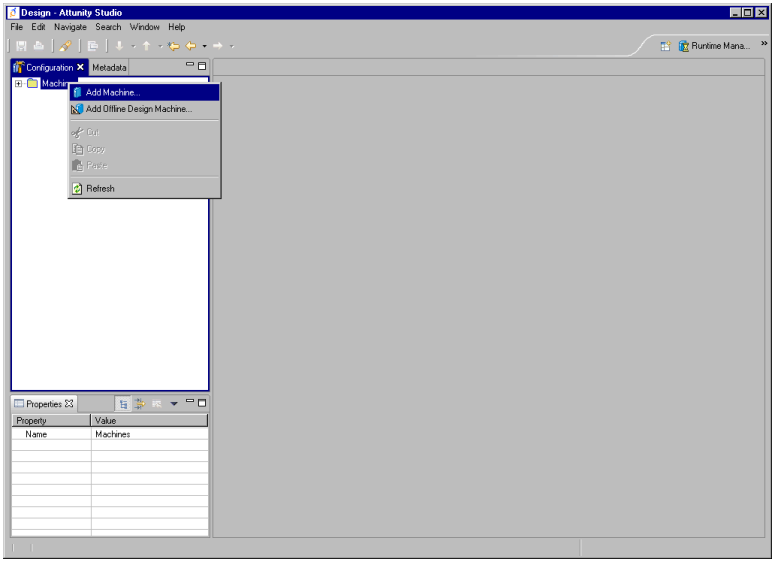
F.1.4 Attunity Studio Configuration

Attunity Studio is used to configure the ODM Server environment from a Windows machine.

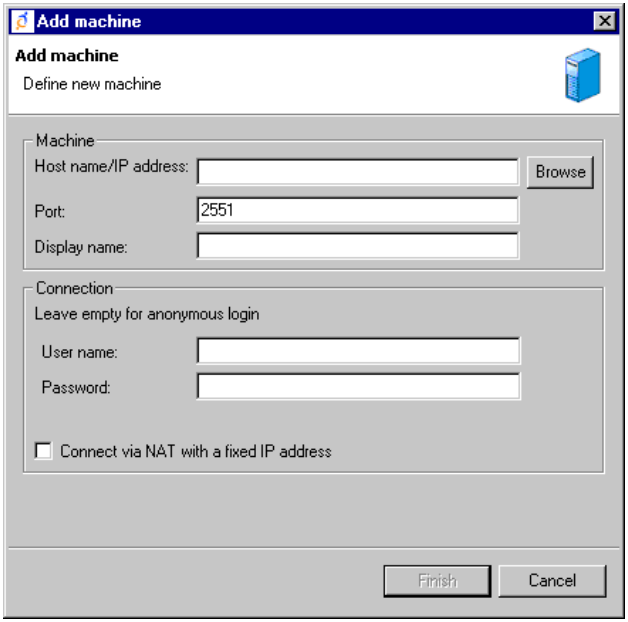
Adding an ODM Server to Attunity Studio

To add an ODM Server to Attunity Studio:

1. Open Attunity Studio from the Attunity folder in the Windows Programs list.
2. In the Configuration explorer, right-click **Machines** and select **Add Machine...** from the shortcut menu to open the **Add machine** dialog.



3. In the **Add machine** dialog, enter the **Host name/IP address** or “localhost” for the machine hosting Attunity Studio.



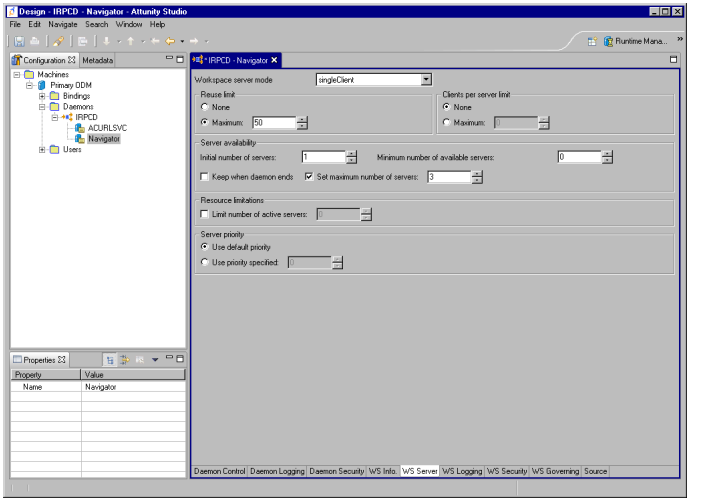
4. Use the default **Port**, 2551.
5. If anonymous logon is not allowed, enter the **User name** and **Password** needed to connect to the machine.

Edit Windows Workspace Server

An ODM Server on a Windows machine must be configured to run a separate process each time ODM accesses an Archive File. This configuration is the default for UNIX servers and no special configuration is required.

To edit the server configuration for Windows:

1. In the Attunity Studio Configuration explorer **Machines** list, expand the Windows server list, the **Daemons** list, and the **IRPCD** list to display the **Navigator** member.
2. Right-click **Navigator** and select **Edit Workspace** from the shortcut menu to open the **IRPCD - Navigator** dialog.



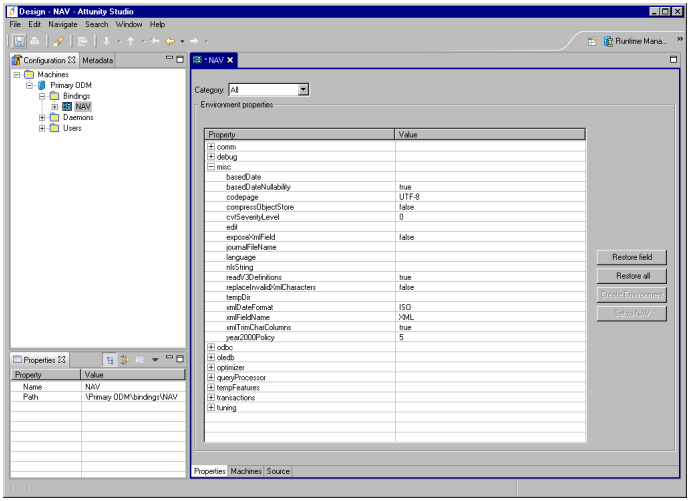
3. Select the **WS Server** tab.
4. From the **Workspace server mode** list, select **singleClient**.
5. From the **File** menu, select **Save All**.

Edit the ODM Server Code Page

UTF-8 users must edit the ODM Server code page. By default, ODM first translates archived data to match the workstation code page on the primary ODM Server. It then translates the code page on the secondary ODM Server (if one exists). You can use UTF-8 data only if all data passed to ODM is in UTF-8 format (including SQL statements). To use UTF-8 format, you must set the code page on the primary and secondary servers.

To edit the ODM Server code page:

1. In the Attunity Studio Configuration explorer **Machines** list, expand the ODM Server list and the **Bindings** list to display the **NAV** member.
2. Right-click the **NAV** member and select **Edit Binding** from the shortcut menu to open the NAV binding editor.



3. Select the **Properties** tab.
4. Expand the **misc** list.
5. From the **codepage** list, select **UTF-8**.
6. From the **File** menu, select **Save All**.

F.2 Define the ODM Data Source on the Primary Server

A data source definition on the primary server is needed to access archived data. You can define a data source for each Archive File and Archive File Collection or specify the Archive File or Archive File Collection in an ODBC or JDBC connection string (see **F.6 Runtime Connection Information**). Procedures for defining a data source on a secondary server are described in **F.3 Secondary Server Configuration**.

Conventions

The conventions used to describe these statements are:

KEYWORD	Keywords are shown in uppercase for emphasis, but can be specified in lower or mixed case.
text	Variable text is shown in lowercase italics.
[ ]	An optional keyword or argument is shown in bolded square brackets.
{ }	A choice of settings from which only one must be selected is shown in bolded curved brackets.
|	Separates options.

Data Source Definition

A data source definition is expressed in XML as follows:

```
<DATASOURCE
      NAME='datasourcename'
      TYPE='PST_GDB' READONLY='true'>
    <CONFIG DIRDB='pstdirectoryname'
        { ARCV_FILE='archivefilename' |
          ARCV_GUID='{gggggg}' | ARCV_ID='n' |
          COLLECTION='archivefilecollection' }
            [ PST_AF_SUBSET={ 'AF_IN(n,n,...)' |
              'AF_DATE_RANGE
              (yyyy-mm-dd-hh:mm:ss,yyyy-mm-dd-hh:mm:ss)' |
              'AF_ID_RANGE(x,y)' } ]
        [ PSTTRACE=COMP (n n ...) [ COMP (n n ...) ] ] />
</DATASOURCE>
```

Syntax

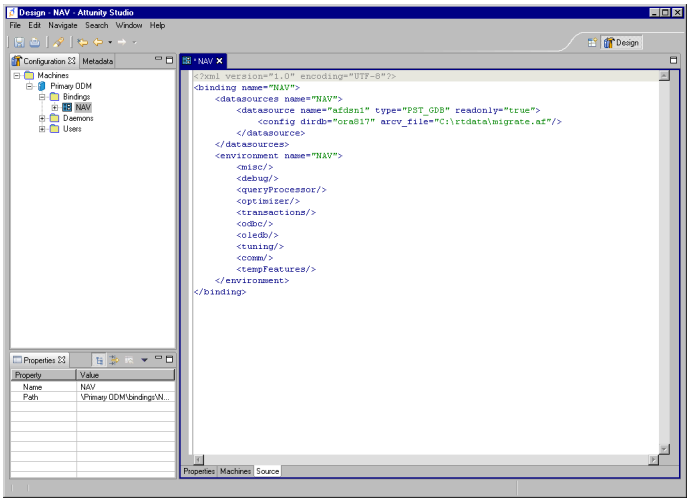
Use the following syntax to define a data source:

<DATASOURCE>	Specifies the name and type of the data source and information required to connect to the data source.
NAME= '*datasourcename*'	The data source name, which can be up to 32 characters and cannot include hyphens ("-").
TYPE= 'PST_GDB'	The data source driver. The value for the ODM driver is 'PST_GDB'.
READONLY= '*true*'	The value for an Archive File or Archive File Collection is 'true.'
<CONFIG>	Specifies configuration properties of a data source.
DIRDB= '*pstdirectoryname*'	The name of the ***Optim*** Directory in which the Archive File or Archive File Collection is registered. Standard ***Optim*** processing opens the ***Optim*** Directory, either reading a configuration file or obtaining Windows registry information. After the ***Optim*** Directory is open, the Archive File or Archive File Collection is validated.
ARCV_FILE= '*archivefilename*'	The fully qualified Archive File name.
ARCV_GUID= '{*gggggg*}'	The Archive File GUID. This value is expressed between curved brackets '{ }'.
ARCV_ID='*nn*'	The Archive File ID number.
COLLECTION= '*archivefilecollection*'	The Archive File Collection name.
PST_AF_SUBSET= '*AF_IN*' | '*AF_DATE_RANGE*' | '*AF_ID_RANGE*'	Subsets an Archive File Collection to specific Archive Files. Use one of the following parameters:

	'**AF_IN**(*n,n,...*)'	Archive Files to include, where *n* is an Archive File name, GUID, or Archive File ID. If a specified Archive File cannot be found, the process will fail.
	'**AF_DATE_RANGE** (*yyyy-mm-dd-hh:mm:ss*, *yyyy-mm-dd-hh:mm:ss*)'	A range of Archive File creation dates. You must include the time of day (hh:mm:ss). You can use zeros for the time (e.g., 00:00:00).
	'**AF_ID_RANGE** (*x,y*)'	A range of Archive File IDs, where *x* is the start and *y* is the end.
PSTTRACE= *COMP (n n ...)*	An optional attribute for turning on the ***Optim*** Trace file. This attribute should be used at the direction of ***Optim*** support. Do not use commas in the PSTTRACE attribute.	

To define an ODM data source:

1. In the Attunity Studio Configuration explorer **Machines** list, expand the primary ODM Server list and the **Bindings** list to display the **NAV** member.
2. Right-click the **NAV** member and select **Edit Binding** from the shortcut menu to open the NAV binding editor.



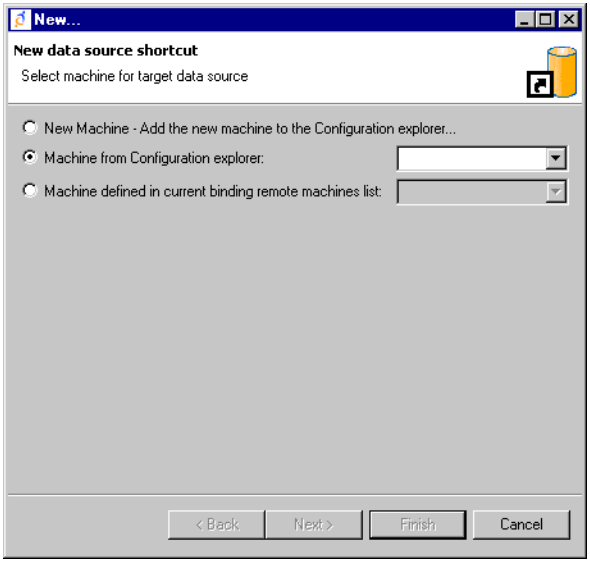
3. Select the **Source** tab.
4. Edit the <datasource> statement to name the data source.
5. Edit the <config> statement to identify an Archive File or Archive File Collection and the ***Optim*** Directory in which it is registered.
6. From the **File** menu, select **Save All**.

F.3 Secondary Server Configuration

An ODM Server must be installed on each workstation that uses ODBC to access ODM data sources. Each data source defined on the primary server must be redefined on the secondary server. This section discusses how to define a data source on the secondary server by creating a shortcut from the primary server. Before configuring the secondary server, you must define it to Attunity Studio, following the procedures in **F.1.4 Attunity Studio Configuration**.

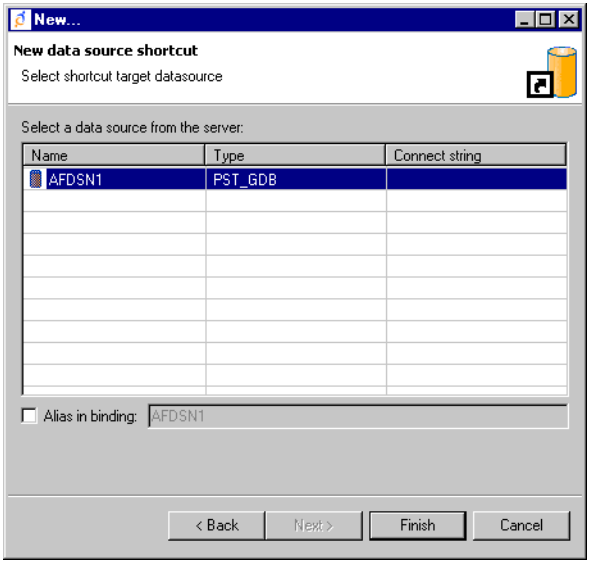
To define data sources on the secondary server:

1. In the Attunity Studio Configuration explorer **Machines** list, expand the secondary ODM Server list, the **Bindings** list, and the **NAV** list to display the **Data sources** member.
2. Right-click the **Data sources** member name and select **New data source shortcut** from the shortcut menu to open the **New data source shortcut** dialog.


New...
New data source shortcut
Select machine for target data source
New Machine - Add the new machine to the Configuration explorer...
Machine from Configuration explorer:
Machine defined in current binding remote machines list:
< Back
Next >
Finish
Cancel

3. Select **Machine from Configuration explorer** and then select the primary server from the corresponding list.

4. Click **Next** until the **New data source shortcut** dialog is displayed.



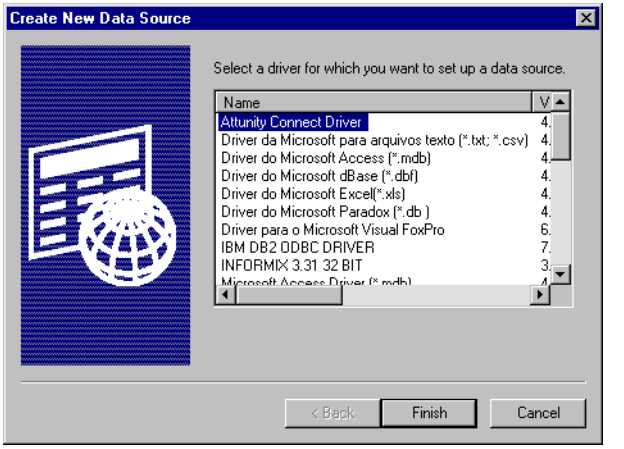
5. Select the data source from the list and click **Finish**.

ODBC Data Source Definition

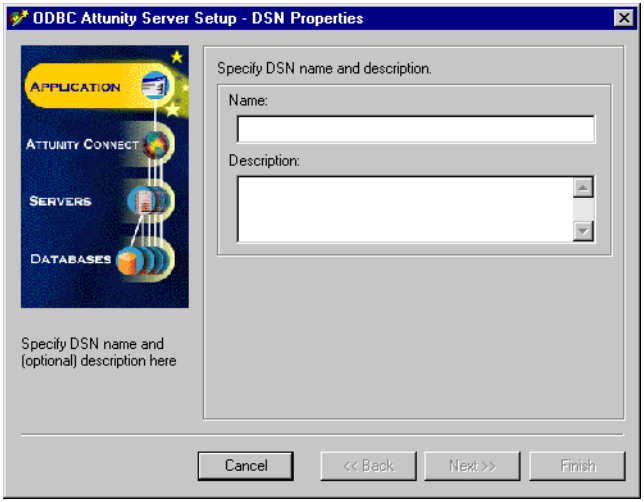
Once the ODM data source shortcut has been created on the secondary ODM Server, you can define the ODBC data source.

To define an ODBC data source on the secondary ODM Server:

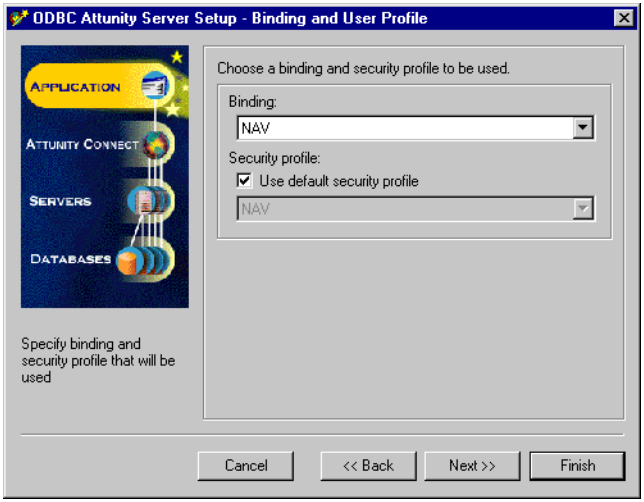
1. From the Administrative Tools in the Windows Control Panel, select **Data Sources (ODBC)** to open the **ODBC Data Source Administrator** dialog.
2. From the **User** or **System** tabs (depending on the data source you want to create), click **Add** to open the **Create New Data Source** dialog.


Create New Data Source
Select a driver for which you want to set up a data source.
Name
Attunity Connect Driver
Driver da Microsoft para arquivos texto (*.txt; *.csv)
Driver do Microsoft Access (*.mdb)
Driver do Microsoft dBase (*.dbf)
Driver do Microsoft Excel(*.xls)
Driver do Microsoft Paradox (*.db)
Driver para o Microsoft Visual FoxPro
IBM DB2 ODBC DRIVER
INFORMIX 3.31 32 BIT
< Back
Finish
Cancel

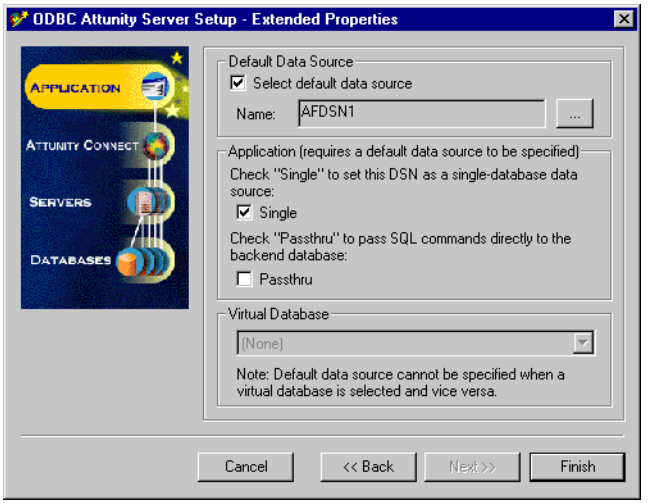
3. Select the Attunity Connect Driver, and click **Finish** to open the **ODBC Attunity Server Setup – DSN Properties** dialog.



4. In **Name**, type a name for the ODBC data source, and click **Next** to open the **ODBC Attunity Server Setup – Binding and User Profile** dialog.



5. Select NAV from the **Binding** list, select the **Use default security profile** check box, and click **Next** to open the **ODBC Attunity Server Setup – Extended Properties** dialog.



6. Select the **Select default data source** check box, click the browse button, and select the data source from the **Browse for Data Source** dialog. Click **OK** to return to the **ODBC Attunity Server Setup – Extended Properties** dialog.
7. Select the **Single** check box, and click **Finish**.

F.4 Thin Client Installation

ODM is shipped with ODBC and JDBC Thin Client packages to provide specific, scalable alternatives to a full server installation on each desktop. These client options provide the flexibility to implement ODM with the desired combination of desktop drivers, but without having to set up a full-scale Attunity environment.

Note: An Attunity license is not required to install the ODBC or JDBC Thin Client.

F.4.1 ODBC Thin Client

The ODBC Thin Client is required on each machine that uses ODBC to connect to ODM. To install the ODBC Thin Client, run the *ThinODBC_V4800_Win32.zip* installation file, located in the ODM\install subdirectory of the ***Optim*** installation directory. Refer to the **Attunity ODBC Thin Client Installation and Guide**, located in the ODM\doc subdirectory of the ***Optim*** installation directory, for more detailed information on installing and using the ODBC Thin Client.

F.4.2 JDBC Thin Client

The JDBC Thin Client is required on each machine that uses JDBC to connect to ODM. To install the JDBC Thin Client, run the *ASTH4820-win32.exe* installation file, located in the ODM\install subdirectory of the ***Optim*** installation directory.

F.5 ODM Security

This section describes a method for securing an ODM environment that uses a primary and secondary server. Using a secondary server is required for ODBC users only. Securing an ODM environment requires the following:

- Providing Archive File Security user credentials on the primary server for each data source.
- Securing the Attunity daemon on both servers.
- Providing administrative authorization for both servers.
- Providing user credentials for secondary server access to the primary server.

Credential Definition

All credentials specified for Attunity authentication are operating system credentials of the machine performing the authorization. For UNIX or Linux, groups as well as individual users are supported. For Windows, groups are not supported and all credentials are based on local users; however, Attunity daemon access can be qualified by domain name (see page 551).

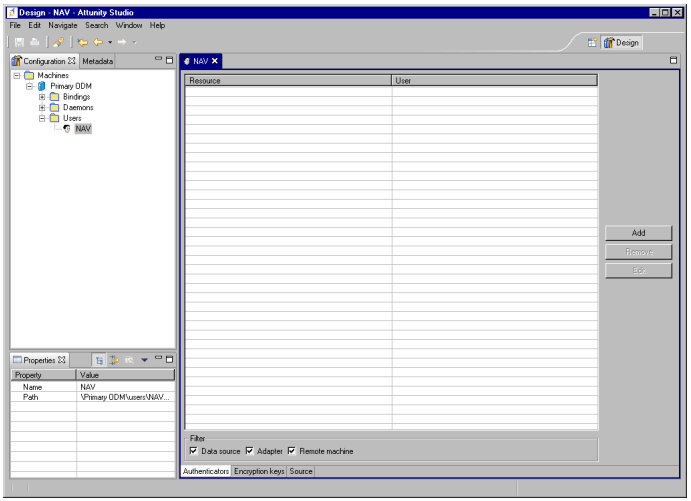
Providing Archive File Security Credentials

Archive File Security user credentials for each data source are assigned to the NAV user profile on the primary server.

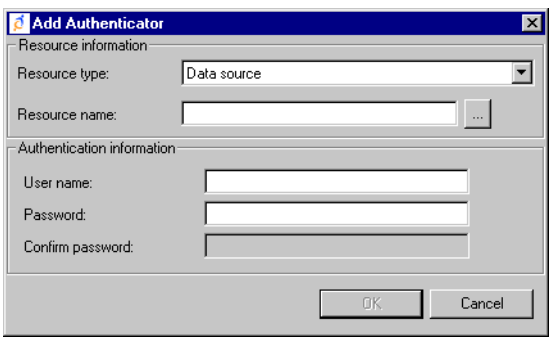
You can also provide Archive File Security credentials in an ODBC or JDBC connection string. For more information, see **F.6 Runtime Connection Information**.

To provide Archive File Security user credentials:

1. In the Attunity Studio Configuration explorer, expand the primary server list and the **User** list to display the **NAV** member.
2. Right-click the **NAV** member and select **Edit User** from the shortcut menu to open the user profile editor.



3. Select the **Authenticators** tab.
4. Click **Add** to open the **Add Authenticator** dialog.



5. In **Resource type**, select Data source.
6. In **Resource name**, type the data source name or use the browse button to select a name.
7. In **User name**, type the user ID with Archive File Security privileges for the data source.

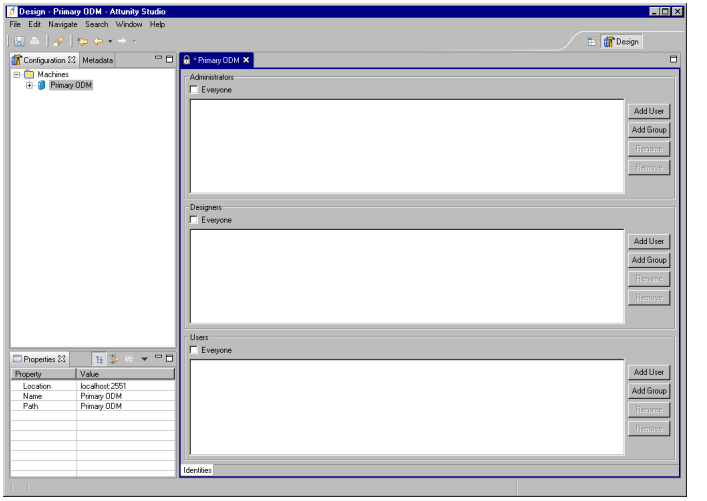
8. In **Password** and **Confirm password**, type the password for the user ID.
9. Click **OK**.
10. From the **File** menu, select **Save All**.

Providing Administrative Authorization for the ODM Server

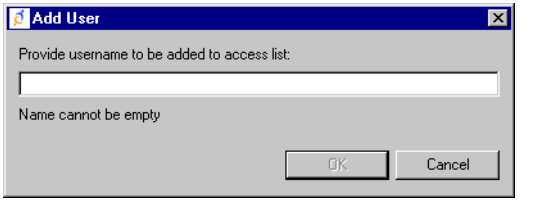
Administrative authorization for an ODM Server controls the ability to modify the server. Perform this step on the primary and secondary servers.

To provide administrative authorization:

1. In the Attunity Studio Configuration explorer, right-click the ODM Server name and select **Administration Authorization** from the shortcut menu to open the administration authorization editor.



2. Clear the **Everyone** check boxes.
3. In the **Administrators** section, click **Add User** to open the **Add User** dialog. (To add a group, click **Add Group**.)



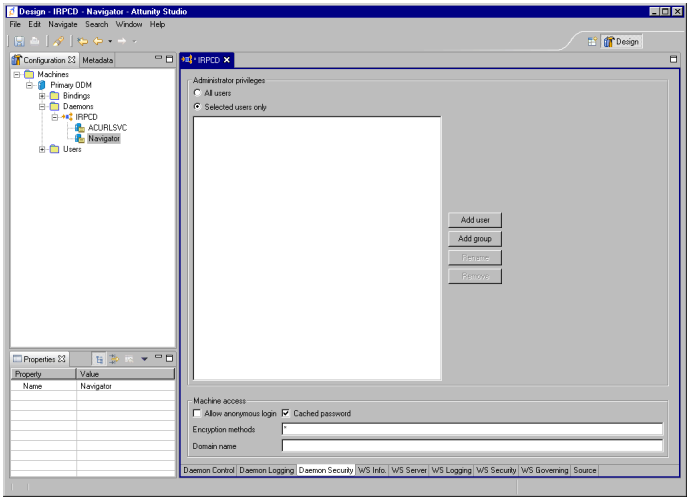
4. Type the user ID or group name that will have administrative privileges for the server.
5. Click **OK**.
6. From the **File** menu, select **Save All**.

Securing the Attunity Daemon

To secure the Attunity daemon, assign machine access and administrator privileges to the daemon. Administrator privileges allow a user to start or stop the daemon. Machine access privileges determine if a user ID and password are required to use the daemon. You must also assign access and administrator privileges to the daemon workspace. These privileges determine the users that can use and administer the workspace. Secure the daemon on the primary and secondary servers.

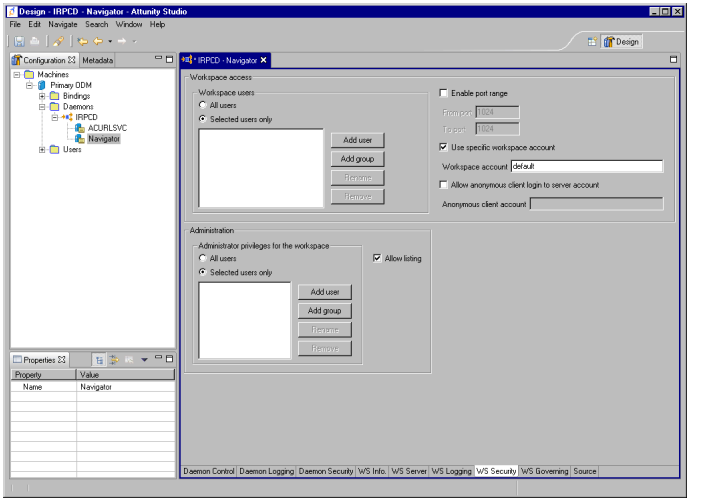
To secure the Attunity daemon:

1. In the Attunity Studio Configuration explorer, expand the ODM Server list, the **Daemons** list, and the **IRPCD** list to display the **Navigator** member.
2. Right-click the **Navigator** member and select **Edit Workspace** to open the daemon configuration editor.



3. Select the **Daemon Security** tab.
4. In the **Administrator privileges** section, select **Selected users only**.
5. Click **Add User** to open the **Add User** dialog. (To add a group, click **Add Group**.)

6. Type the user ID or group name that will have administrative privileges for the daemon.
7. Click **OK**.
8. In the **Machine access** section, clear the **Allow anonymous login** check box.
9. For Windows only. Use **Domain name** to qualify user names with a domain name.
10. Select the **WS Security** tab.



11. In the **Workspace users** section, select **Selected users only**.
12. Click **Add User** to open the **Add User** dialog. (To add a group, click **Add Group**.)
13. Type the user ID or group name that will have user privileges for the workspace.
14. In the **Administrator privileges for the workspace** section, select **Selected users only**.
15. Click **Add User** to open the **Add User** dialog. (To add a group, click **Add Group**.)
16. Type the user ID or group name that will have administrative privileges for the workspace.
17. From the **File** menu, select **Save All**.

Secondary Server Access to the Primary Server

Secondary servers require credentials to access the primary server. These credentials are assigned to the NAV user profile on the secondary server.

To provide credentials for secondary server access:

1. In the Attunity Studio Configuration explorer, expand the secondary server list and the **User** list to display the **NAV** member.
2. Right-click the **NAV** member and select **Edit User** from the shortcut menu to open the user profile editor.
3. Select the **Authenticators** tab.
4. Click **Add** to open the **Add Authenticator** dialog.
5. In **Resource type**, select Remote machine.
6. In **Resource name**, type the primary server name and, preceded by a colon, the port number for the Attunity daemon on the primary server. For example, *machinename:port*.
7. In **User name**, type the user ID with privileges to access the primary server.
8. In **Password** and **Confirm password**, type the password for the user ID.
9. Click **OK**.
10. From the **File** menu, select **Save All**.

F.6 Runtime Connection Information

The **Attunity Connect Guide and Reference** manual, located in the *AC_DOC.pdf* file in the ODM\doc subdirectory of the ***Optim*** installation directory, specifies the format and contents of the connection strings for ODBC and JDBC. An Archive File or Archive File Collection specified in the connection string overrides the corresponding specification in the ODM data source definition. If an Archive File or Archive File Collection is not identified in the data source, you must specify an Archive File or Archive File Collection in the connection string.

Connection Parameters

The following are special connection parameters that can be used when connecting to an ODM data source from ODBC or JDBC:

```
DSNCONFIG=datasourcename1( [ ARCV_FILE=archivefilename |
    ARCV_GUID=gggggg | ARCV_ID=n
    | COLLECTION=archivefilecollection ] ,
      [ PST_AF_SUBSET={ 'AF_IN(n,n,...)' |
        'AF_DATE_RANGE
        (yyyy-mm-dd-hh:mm:ss,yyyy-mm-dd-hh:mm:ss)' |
        'AF_ID_RANGE(x,y)' } ]
    [ PSTTRACE=COMP (n n ...) [ COMP (n n ...) ] ] )
    & datasourcename2(...)

DSNPASSWORDS=datasourcename=domainname/userID/
    password & datasourcename2=...

QPTDPNAME=primaryservername:daemonportnumber
```

Note: For additional connection parameters, refer to Attunity documentation.

DSNCONFIG= *datasourcename* — The ODM data source name.

ARCV_FILE= *archivefilename* — The fully qualified Archive File name.

ARCV_GUID= *gggggg* — The Archive File GUID.

ARCV_ID=*n* — The Archive File ID number.

COLLECTION= *archivefilecollection* — The Archive File Collection name.

PST_AF_SUBSET= '*AF_IN*' | '*AF_DATE_RANGE*' | '*AF_ID_RANGE*'	Subsets an Archive File Collection to specific Archive Files. Use one of the following parameters:	
	'**AF_IN**(*n,n,...*)'	Archive Files to include, where *n* is an Archive File name, GUID, or Archive File ID. If a specified Archive File cannot be found, the process will fail.
	'**AF_DATE_RANGE** (*yyyy-mm-dd-hh:mm:ss*, *yyyy-mm-dd-hh:mm:ss*)'	A range of Archive File creation dates. You must include the time of day (hh:mm:ss). You can use zeros for the time (e.g., 00:00:00).
	'**AF_ID_RANGE** (*x,y*)'	A range of Archive File IDs, where *x* is the start and *y* is the end.
PSTTRACE= *COMP (n n ...)*	An optional attribute for turning on the ***Optim*** Trace file. This attribute should be used at the direction of ***Optim*** support. Do not use commas in the PSTTRACE attribute.	
DSNPASSWORDS= *datasourcename= domainname/ userID/ password*	The user ID and password for Archive File Security authentication. The *datasourcename* is the data source to which the credentials apply. The *domainname* is optional. You can use forward or backward slashes within the parameter. If this parameter is not used, the credentials of the user running the Attunity Server will be used for Archive File Security authentication.	
QPTDPNAME= *primaryservername: daemonportnumber*	The primary server name and port number of the Attunity daemon on the primary server. Required when the connection string is passed from a secondary server.	

F.7 ODM Data Type Conversions

The following data type conversions occur when Archive File data is accessed by ODM:

- When code page translation of archived data to UTF-8 is required, character column length may be extended 1.5 times for NCHAR data or 3 times for single byte character data, up to 32k. However, if the total row size is greater than 32k, ODM may encounter errors when joining or sorting data.
- VARBINARY columns are converted to BINARY columns. The BINARY column data is padded with binary zeros to match the VARBINARY column maximum data length. (For DB2 LUW, the data is padded with ASCII spaces, x'20'.)
- For MONEY, DECIMAL, or NUMERIC columns, if scale=0, these data types are converted to int2 or int4. If precision <=31 and both scale>=0 and scale<=precision, these data types are converted to NUMERIC(p,s), otherwise they are converted to BINARY_DOUBLE.
- NCLOBs are converted to CLOBs.
- For Oracle, NUMERIC columns without precision are converted to BINARY_DOUBLE.

  Timestamps (including TZ and LZ) are converted to ODBC timestamps.
- For Oracle and Informix, time intervals are converted to VARCHAR(30).
- For DB2 LUW, LONGVARCHAR, LONGVARBINARY and LONGVARGRAPHIC columns are converted to CLOBs or BLOBs.

F.8 Archive File to XML Convertor

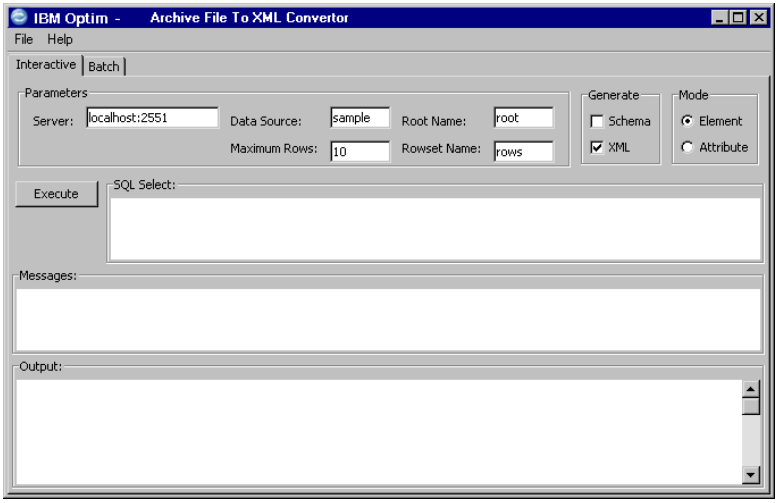
Use the **Archive File to XML Convertor** to convert Archive File data to XML format. You can identify the data to convert by typing SQL SELECT statements or using a batch file. You can also create a file that includes an XML schema describing Archive File data.

The **Archive File to XML Convertor** requires Java JRE release 1.4 or later. To open the **Archive File to XML Convertor**, run the *atoxml.jar* executable file, located in the ODM\java subdirectory of the ***Optim*** installation directory.

For batch and command line documentation, refer to the **Archive File to XML Convertor** online help, available from the **Help** menu.

Interactive Tab

Use the **Interactive** tab to type an SQL STATEMENT that specifies the data to convert.



Parameters

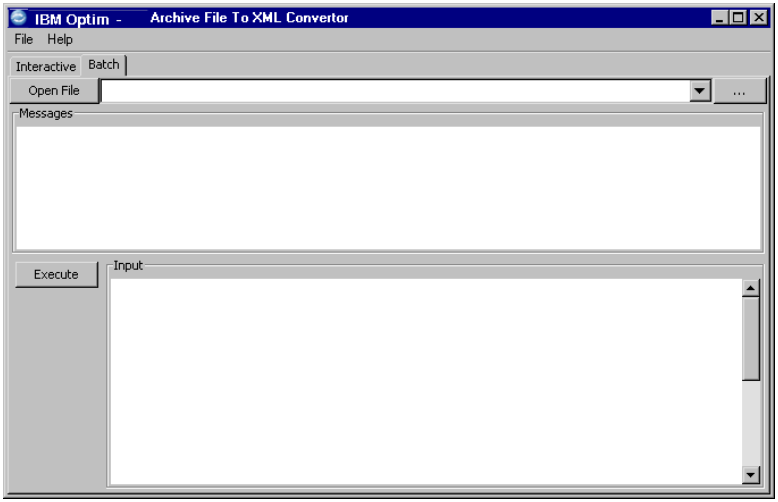
Server — The machine name of the ODM Server, followed by a colon ":" and the port number. If the default port number (2551) is used, the port number can be omitted.

Data Source — The data source for the Archive File.

	Maximum Rows	The maximum number of rows to convert to XML.
	Root Name	The name of the root XML tag.
	Rowset Name	The name of the XML tag in which the data is placed.
Generate		
	Schema	Select this check box to include XML schema of the Archive File data with the output XML.
	XML	Select this check box to include Archive File data with the output XML.
Mode		
	Element	Select this check box to generate an XML tag for each data value.
	Attribute	Select this check box to generate <row> tag attributes for each data value.
Execute	Click to begin the conversion process.	
SQL Select	Type an SQL SELECT statement to specify selection criteria for the data.	
Messages	Displays messages for the conversion process.	
Output	Displays the XML output.	

Batch Tab

Use the **Batch** tab to specify the data to convert by using a batch file or typing batch parameters.



Open File Click to select a batch input file.

Messages Displays message for the conversion process.

Execute Click to execute the batch process.

Input Type the batch parameters, if a batch input file is not used.

Conversion Issues

The following issues arise in the conversion of archived data to XML:

- Characters that are not legal in XML, including characters less than x'20' (except for carriage return, linefeed, and tab), are replaced by a '?'. A diagnostic is written when this occurs.
- CLOBs (character large objects) are written as single long lines.
- Binary data is encoded as base64 data and written as single long lines.
- Null columns are omitted in attribute mode and indicated by xsi:nil="true" in element mode. Note that because of a limitation in the Attunity interface, null large objects are given zero length; they are not marked explicitly as null.

- Characters in the first column of the following table are translated to the entity reference in the second column:

Character	Entity Reference
“	"
&	&
‘	'
<	<
>	>

F.9 Archive File Collections

An Archive File Collection is a list of Archive Files that can be logically unioned together as a single data source for ODM access. For example, ODM uses an Archive File Collection to provide access to data in multiple Archive Files, even if all files do not include a specific table or column or if the attributes of data in a column vary from file to file. ODM processes Archive Files in the order they are listed in the **Archive File Collection Editor**. For information about creating Archive File Collections, refer to the ***Archive* User Manual, 9.4 Archive File Collections**.

Unioned Tables

Tables with matching creator IDs and names in separate Archive Files will be unioned. To be processed, a table need not exist in every Archive File. ODM is not case-sensitive. ODM does not use DB Aliases; however, an Archive File cannot have two tables with matching creator IDs and names but different DB Aliases.

Matching tables are not required to have the same columns. The union will include all column names in the matching tables. Rows from a table that do not include a column found in another table will use a default value such as NULL, a default date specified in the **Archive File Collection Editor**, or an appropriate data type (spaces, zero, etc.).

Column Compatibility

All columns with the same name that are in tables with matching creator IDs and names must have compatible attributes. If columns have different but compatible attributes, a compatible attribute will be used for those columns. The column compatibility rules for the Compare Process apply to Archive File Collections. For information about comparison compatibility rules, refer to the **Common Elements Manual, 5.3.1 Comparison Compatibility Rules**.

For example, columns COLX DECIMAL(8,2) and COLX DECIMAL(10,0) will become COLX DECIMAL(10,2).

If a compatible attribute cannot be found (e.g., COLX INTEGER and COLX TIMESTAMP), the **Archive File Collection Editor** will display an error message.

Unioned Indexes

Archive Indexes for unioned tables may also be unioned. The following rules apply to unioned indexes:

- Each Archive File that includes the table must also include the index.

- ODM will use a unioned index until a column with a different name or attribute is found (compatible attributes are not used). The unique column and remaining columns in the index will not be processed.

Archive File Security

If Archive File Security denies you access to a table or a column in table, no rows are retrieved from the table.

F.9.1 Archive File Collection Subsets

You can specify a subset of files in an Archive File Collection using a data source definition (see page 538), connection string (see page 554), or SQL WHERE clause.

The PST_AF_SUBSET pseudocolumn is logically added to each archived table during ODM processing and allows you to create a subset using an SQL WHERE clause. Use the following syntax:

PST_AF_SUBSET='*AF_IN(n,n...)*' | '*AF_ID_RANGE(x,y)*' | '*AF_DATE_RANGE(yyyy-mm-dd-hh:mm:ss,yyyy-mm-dd-hh:mm:ss)*'

'AF_IN(*n,n,...*)'	Archive Files to include, where *n* is an Archive File name, GUID, or Archive File ID.
'AF_ID_RANGE(*x,y*)'	A range of Archive File IDs, where *x* is the start and *y* is the end.
'AF_DATE_RANGE (*yyyy-mm-dd-hh:mm:ss*, *yyyy-mm-dd-hh:mm:ss*)'	A range of Archive File creation dates. You must include the time of day (hh:mm:ss). You can use zeros for the time (e.g., 00:00:00).

The subset criteria need only be specified once in an SQL statement. If subset criteria is specified in the data source or connection string, the WHERE clause subset must be a subset of that criteria.

F.9.2 PST_ARCHIVE_ID Pseudocolumn

The PST_ARCHIVE_ID pseudocolumn is logically added to each archived table during ODM processing and contains the Archive File ID of the Archive File that includes the table. Use PST_ARCHIVE_ID to specify the Archive File from which a row is selected.

For example, you can use PST_ARCHIVE_ID to control a join by avoiding duplicate rows from a table in multiple files in the Archive File Collection. If the DETAILS table is related to the ITEMS table, and only the DETAILS table is unique across all files in the collection, then a join between the tables would result in duplicate ITEMS rows joined with DETAILS rows. To avoid duplicate rows, use the following syntax:

```
SELECT * FROM PST.DETAILS, PST.ITEMS
WHERE
PST.DETAILS.ITEM_ID=PST.ITEMS.ITEM_ID
AND
PST.DETAILS.PST_ARCHIVE_ID=PST.ITEMS.PST_ARCHIVE_ID
```

F.9.3 PST_ARCHIVE_FILES Table

An Archive File Collection includes a table named PST_ARCHIVE_FILES, which contains a row for each Archive File in the collection. PST_ARCHIVE_FILES has the following columns:

Column Name	Data Type	Description
ARCHIVE_ID	INTEGER	Archive File ID
GUID	CHAR(40)	Archive File GUID
ARCHIVE_FILE_NAME	VARCHAR(256)	Archive File name
ARCHIVE_DATETIME	TIMESTAMP	Archive File creation date and time

You can use this table to query context data from the Archive Files in the collection. For example, use the following syntax to find the latest Archive File ID:

```
SELECT MAX(ARCHIVE_ID) FROM PST_ARCHIVE_FILES
```

Appendix G. Converting PST and Optim Directory Objects

All PST Directories created prior to version 6.0 of the Princeton Softech products, ***Archive*** and the ***Relational Tools***, require a conversion to be compatible with later versions. Additionally, any ***Optim*** Directory created prior to ***Optim*** version 6.2 on an SQL Server database must be converted.

Use the Configuration program to convert ***Optim*** Directories and objects. After the Conversion Process, your "old" PST Directory and objects remain intact and can still be used with the ***Optim*** products.

Version 5.x PST Directories

PST Directory objects created using version 5.x of ***Archive*** or the ***Relational Tools*** must be converted into a format suitable for use with version 6.0 or later. Use the Conversion Process in the **Configuration** program to migrate objects from an old (5.x) PST Directory to a Directory compatible with version 6.0 or later.

You can convert and migrate the following objects: Access Definitions, Table Maps, Column Maps, Column Map Procedures, Primary Keys, DB Aliases, Relationships, Calendars, Currency Definitions, Storage Profiles, process requests, Archive File Directory entries, and File Access Definitions.

Note: When running setup, select the **5.x PST Directory Conversion** component to install files required for converting PST Directory objects.

The Conversion Process consists of three steps, which must be completed in the order listed.

1. Create a new ***Optim*** Directory. This step can be completed prior to running the Conversion Process, if desired, using commands available from the **Tasks** menu.

Note: If you create a new Directory before using the Conversion Process, note the following:

- If Object Security is applied to a 6.0 Directory before you convert 5.x objects, you can automatically secure converted objects. Automatically securing objects may be more convenient than securing each object manually. For more information, see **Automatically Associate an Object with an ACL** on page 469.
- If Functional Security is enabled for the 6.0 Directory, you must have the create privilege for the objects you are converting. For more information, see **Functional Privileges Tab** on page 458.

2. Export objects from the old PST Directory to an Export File.
3. Import objects from the Export File to the new ***Optim*** Directory. You can complete this step from any workstation having access to the new ***Optim*** Directory and Export File.

If you have upgraded your DBMS, or if imported DB Aliases reference a DBMS version that is no longer supported by ***Optim***, you must run the **Update the DBMS Version for a DB Alias** configuration task after converting the PST Directory.

Version 6.0/6.1 PST Directories on SQL Server

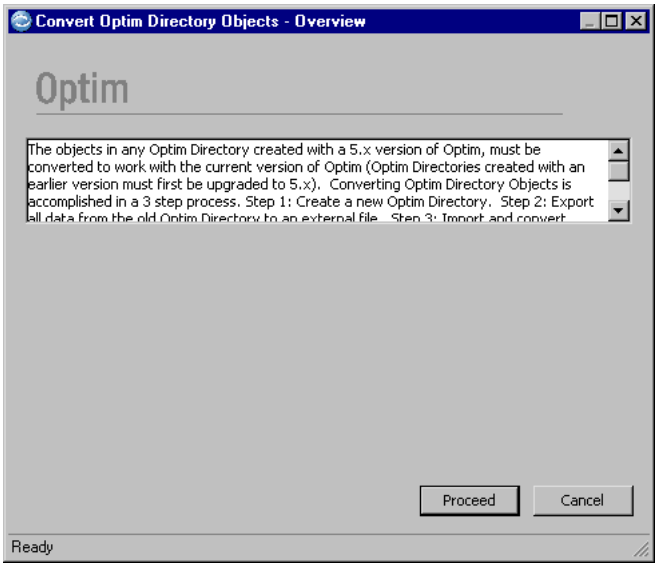
PST Directory tables created with the Princeton Softech products versions 6.0/6.1 in an SQL Server database must be converted to accommodate Unicode support in later versions of ***Optim***. The Directory conversion process will copy data in 6.0/6.1 Directories to new Directory tables. The new and old Directories will have the same name and PST object definitions. After the Directory is converted, you can still use the old Directory tables with the Princeton Softech products version 6.0/6.1, or you can drop the 6.0/6.1 Directory.

G.1 Conversion Process for 5.x *Optim* Directories

The **Configuration** program presents a series of dialogs that provide instructions to guide you through each step of the Conversion Process. During the process, you make selections appropriate to your particular site and circumstances.

Note: Refer to **4.1.5 Dialogs** on page 73 for details on options that are common to the configuration dialogs.

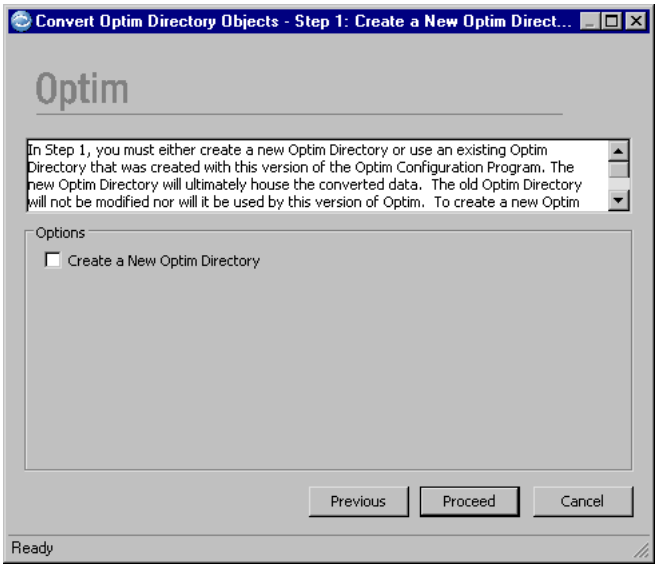
To begin the process, select **Convert Optim Directory Objects** from the **File** menu. The first window is the **Overview** dialog.


Convert Optim Directory Objects - Overview
Optim
The objects in any Optim Directory created with a 5.x version of Optim, must be converted to work with the current version of Optim (Optim Directories created with an earlier version must first be upgraded to 5.x). Converting Optim Directory Objects is accomplished in a 3 step process. Step 1: Create a new Optim Directory. Step 2: Export
Proceed
Cancel
Ready

Click **Proceed** to continue.

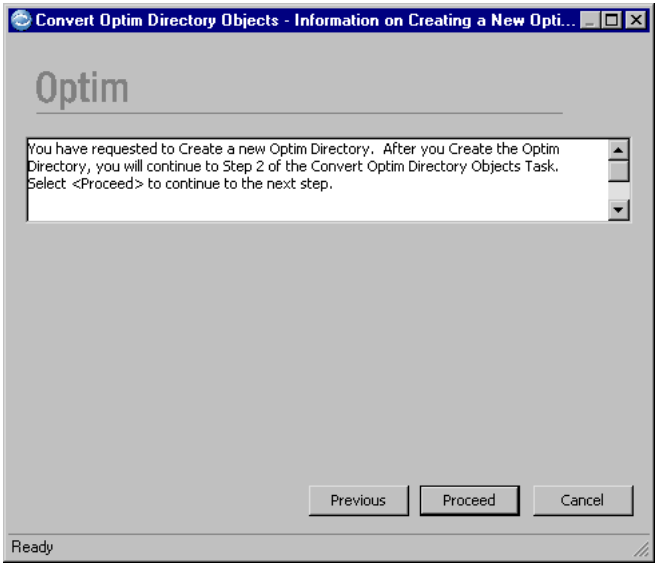
G.1.1 Step 1: Create a New Optim Directory

The next dialog prompts you to create a new ***Optim*** Directory. This Directory will store objects exported from the old Directory.


Convert Optim Directory Objects - Step 1: Create a New Optim Direct...
Optim
In Step 1, you must either create a new Optim Directory or use an existing Optim Directory that was created with this version of the Optim Configuration Program. The new Optim Directory will ultimately house the converted data. The old Optim Directory will not be modified nor will it be used by this version of Optim. To create a new Optim
Options
Create a New Optim Directory
Previous
Proceed
Cancel
Ready

If you created the new ***Optim*** Directory earlier, leave the check box blank and click **Proceed** to display the **Export Data from an Old Optim Directory?** dialog, discussed in **G.1.2 Step 2: Export Data from Old Optim Directory**.

To create a new ***Optim*** Directory, however, select the **Create a New Optim Directory** check box and click **Proceed** to display the **Information on Creating a New Optim Directory** dialog.


Convert Optim Directory Objects - Information on Creating a New Opti...
Optim
You have requested to Create a new Optim Directory. After you Create the Optim Directory, you will continue to Step 2 of the Convert Optim Directory Objects Task. Select <Proceed> to continue to the next step.
Previous
Proceed
Cancel
Ready

From this point, the task is similar to creating an ***Optim*** Directory when configuring the first workstation. These steps are described briefly in the following paragraphs. For further details, refer to **5.1.2 Create Optim Directory** on page 78.

Specify Optim Directory

The first step in creating a new ***Optim*** Directory is to provide the name of the ***Optim*** Directory. The **Configuration** program prompts for this information by presenting the **Specify Optim Directory** dialog. You must select **Create New Optim Directory and Registry Entry** and specify a Directory name.

Note: The name of the new Directory must be different from the name of the old Directory.

Specify Optim Directory DBMS

You must then specify the database in which to create the new ***Optim*** Directory tables. On the **Specify Optim Directory DBMS** dialog, specify the type and version of DBMS software, and optionally, provide a description of the ***Optim*** Directory.

Connect to Database

The **Configuration** program must connect to the database in order to create the new ***Optim*** Directory tables and packages, plans, or procedures. To enable this connection, you must enter a valid **User ID**,

Password, and **Connection String** on the **Connect to Database** dialog. This User ID must have authorization to create tables and catalog stored procedures or bind packages.

Create Optim Directory Tables

After the workstation is connected to the database, you can create the ***Optim*** Directory. The **Configuration** program names the tables automatically, but you can specify the identifier (**Creator ID**, **Owner ID**, or **Schema Name**) and the database tablespace for each table. The **Create Optim Directory Tables** dialog prompts you for the information needed to create these tables.

Create/Drop Packages

Before creating packages, plans, or procedures for the ***Optim*** Directory tables, the **Configuration** program displays the **Create/Drop Packages**, **Create/Drop Stored Procedures**, or **Bind/Drop Plans** dialog, depending on the DBMS selected for the Directory. You can choose to browse the SQL statements generated to create or refresh the packages, plans, or procedures.

Keep Optim Directory Data in Unicode Format

If you are creating a new ***Optim*** Directory in a DBMS for which ***Optim*** provides Unicode support, you are prompted to indicate whether the DBMS is configured to store unicode data.

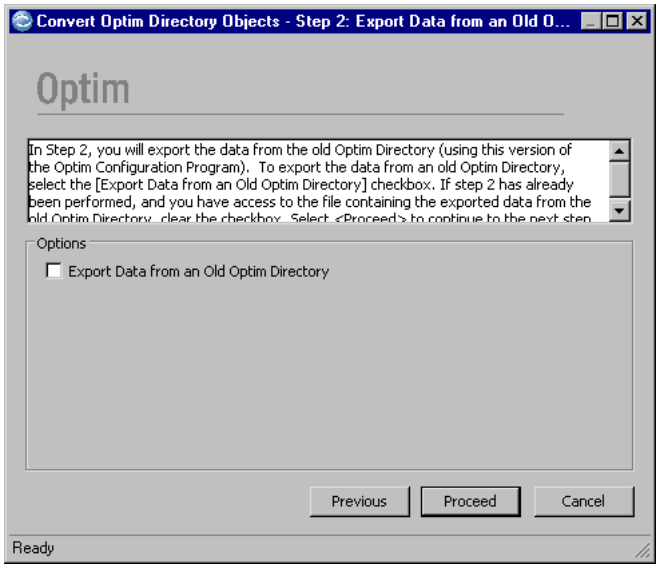
Connect to Database

The **Configuration** program creates a Windows registry entry used to access the ***Optim*** Directory. For subsequent access to the Directory from this workstation, you can use the **Connect to Database** dialog to specify a **User ID** and **Password** different from those used to create the Directory.

After you have created the new ***Optim*** Directory, the Conversion Process displays the **Export Data from an Old Directory** dialog.

G.1.2 Step 2: Export Data from Old *Optim* Directory

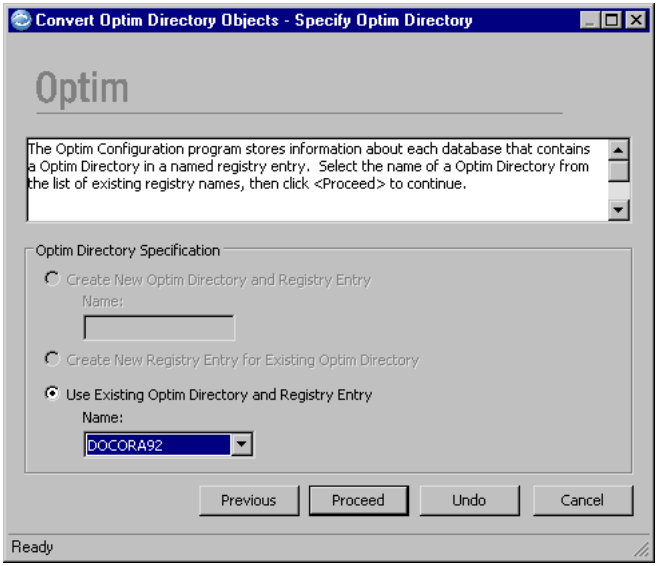
The next step in the process is to export objects from the old ***Optim*** Directory.


Convert Optim Directory Objects - Step 2: Export Data from an Old O...
Optim
In Step 2, you will export the data from the old Optim Directory (using this version of the Optim Configuration Program). To export the data from an old Optim Directory, select the [Export Data from an Old Optim Directory] checkbox. If step 2 has already been performed, and you have access to the file containing the exported data from the
Options
Export Data from an Old Optim Directory
Previous
Proceed
Cancel
Ready

To begin this step, select the **Export Data from an Old Optim Directory** check box and click **Proceed**. To skip this step and display the **Import Data into New Optim Directory?** dialog, leave the check box blank and click **Proceed**.

Specify Optim Directory

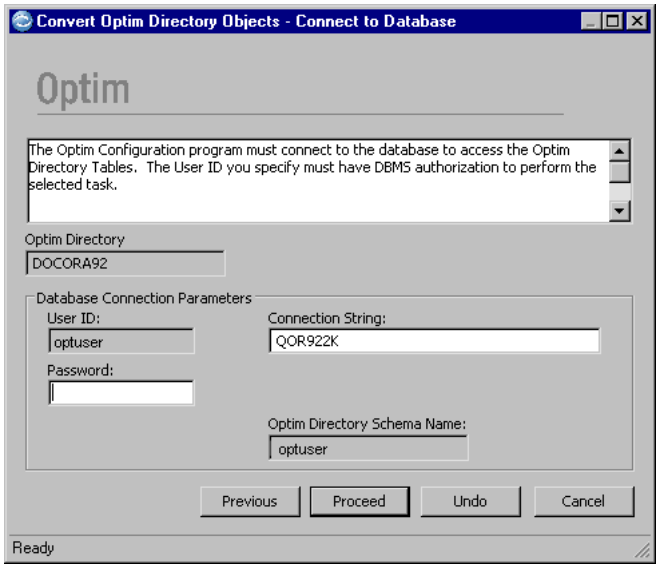
Use the **Specify Optim Directory** dialog to select the name of the ***Optim*** Directory from which objects are exported.


Convert Optim Directory Objects - Specify Optim Directory
Optim
The Optim Configuration program stores information about each database that contains a Optim Directory in a named registry entry. Select the name of a Optim Directory from the list of existing registry names, then click <Proceed> to continue.
Optim Directory Specification
Create New Optim Directory and Registry Entry
Name:
Create New Registry Entry for Existing Optim Directory
Use Existing Optim Directory and Registry Entry
Name:
DOCORA92
Previous
Proceed
Undo
Cancel
Ready

Connect to Database

The **Configuration** program must connect to the database in order to access the old ***Optim*** Directory tables. The entries in the **Connect to**

Database dialog are populated with values entered when the old Directory was created.

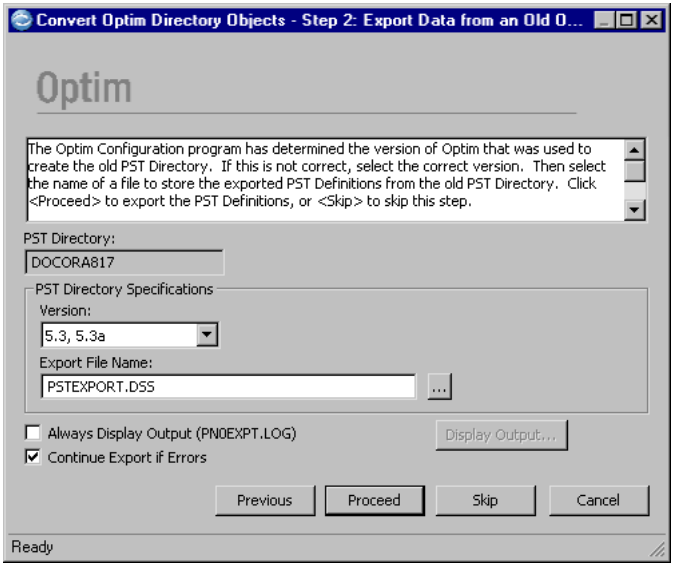


Connection String — The name or string needed for the server to access the ***Optim*** Directory database.

Password — Enter the password (up to 30 characters) that corresponds to the specified User ID.

Export Old Directory Definitions

After the workstation is connected to the database, you can export objects using this dialog.


Convert Optim Directory Objects - Step 2: Export Data from an Old O...
Optim
The Optim Configuration program has determined the version of Optim that was used to create the old PST Directory. If this is not correct, select the correct version. Then select the name of a file to store the exported PST Definitions from the old PST Directory. Click <Proceed> to export the PST Definitions, or <Skip> to skip this step.
PST Directory:
DOCORA817
PST Directory Specifications
Version:
5.3, 5.3a
Export File Name:
PSTEXPORT.DSS
...
Always Display Output (PN0EXPT.LOG)
Display Output...
Continue Export if Errors
Previous
Proceed
Skip
Cancel
Ready

PST Directory

Name of the PST Directory from which objects are exported.

PST Directory Specifications

Version — Version of **Configuration** program used to create the old PST Directory.

Export File Name — Enter the name of the Export File. The Export File is a plain text file and has a .dss extension by default. Other extensions may be specified, or the file can be designated without an extension. The Export File is used as the input for Import Processing.

Always Display Output (PN0EXPT.LOG)

Select the check box to automatically display the export process log for the current process. When the Export Process is complete, the log is displayed in the **Browse File** dialog. To display the log only in the event of an error, clear the check box.

Continue Export if Errors

Indicate whether to halt processing if an error occurs. To continue processing if an error occurs, select the check box. To halt processing if an error occurs, clear the check box.

Run Export

To start the Export Process, click **Proceed**. If you specify the name of an Export File that already exists, a dialog prompts you to confirm that you want to overwrite the file. During Export Processing, the status bar displays information about the process.

If errors occur, processing continues if **Continue Export if Errors** is selected. Errors are written to the export process log after Export Processing is finished. The log is displayed in the **Browse File** dialog. You can review and print the log for diagnostic information about errors.

If some objects fail to be exported due to errors, check the specifications, and try the Export Process again by clicking **Proceed**.

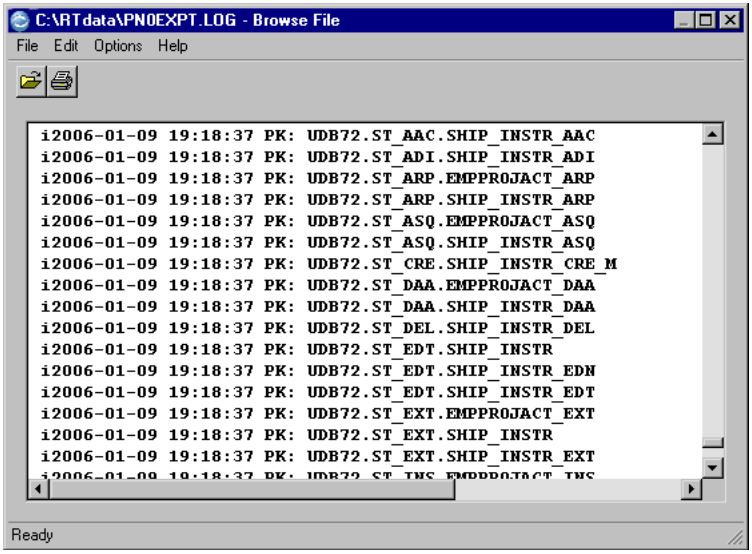
When processing is finished, the status bar displays the message: "Ready."

Browse File

The **Browse File** dialog displays the results of the Export Process, and includes the following details:

- Names of exported objects, grouped by object type.
- Date and time each object was exported.
- Explanatory text for each error, if errors were encountered.

The following is a sample export process log:

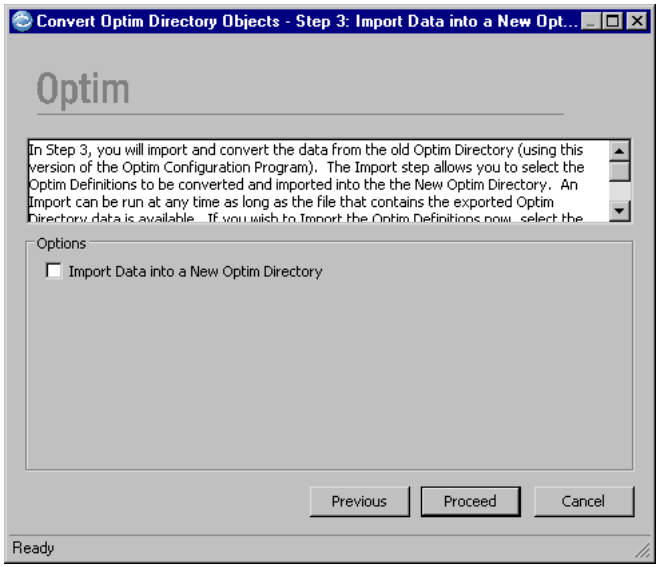


Print the log by choosing **Print** from the **File** menu. Each execution of the Export Process clears the log file before information for the current execution is written. Previous log information is not retained.

Select **Close** from the **File** menu to close the log and return to the **Export** dialog. You can redisplay the log for the current process by clicking **Display Output**.

G.1.3 Step 3: Import Data into New *Optim* Directory

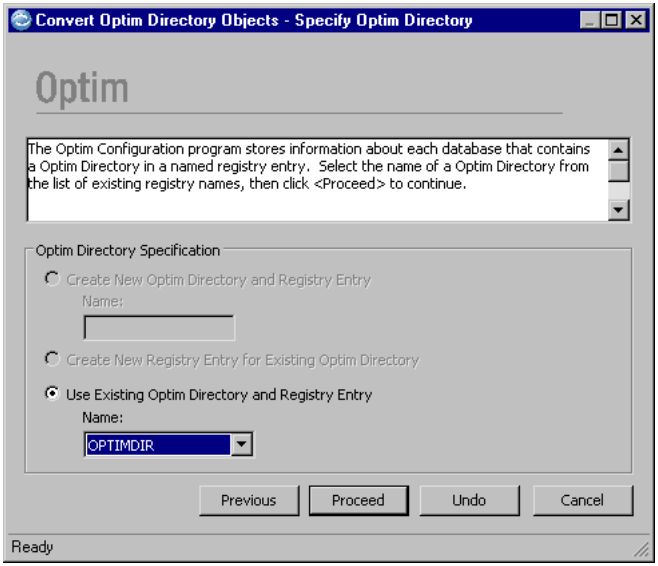
The next step in the Conversion Process is to import the objects into the new ***Optim*** Directory.


Convert Optim Directory Objects - Step 3: Import Data into a New Opt...
Optim
In Step 3, you will import and convert the data from the old Optim Directory (using this version of the Optim Configuration Program). The Import step allows you to select the Optim Definitions to be converted and imported into the the New Optim Directory. An Import can be run at any time as long as the file that contains the exported Optim
Options
Import Data into a New Optim Directory
Previous
Proceed
Cancel
Ready

To begin this step, select the **Import Data into a New Optim Directory** check box and click **Proceed**. To skip this step, leave the check box blank and click **Proceed**.

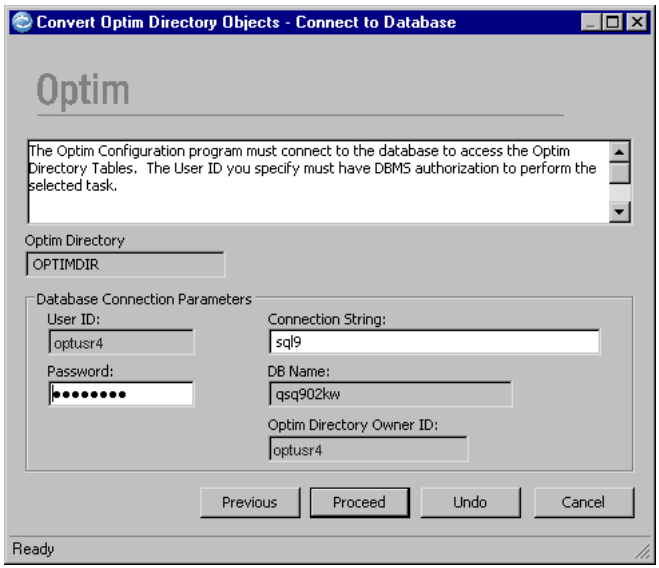
Specify Optim Directory

Use the **Specify Optim Directory** dialog to select the name of the new ***Optim*** Directory into which objects are imported.


Convert Optim Directory Objects - Specify Optim Directory
Optim
The Optim Configuration program stores information about each database that contains a Optim Directory in a named registry entry. Select the name of a Optim Directory from the list of existing registry names, then click <Proceed> to continue.
Optim Directory Specification
Create New Optim Directory and Registry Entry
Name:
Create New Registry Entry for Existing Optim Directory
Use Existing Optim Directory and Registry Entry
Name:
OPTIMDIR
Previous
Proceed
Undo
Cancel
Ready

Connect to Database

The **Configuration** program must connect to the database in order to access the new ***Optim*** Directory tables. The entries in the **Connect to Database** dialog are populated with values entered when the Directory was created.

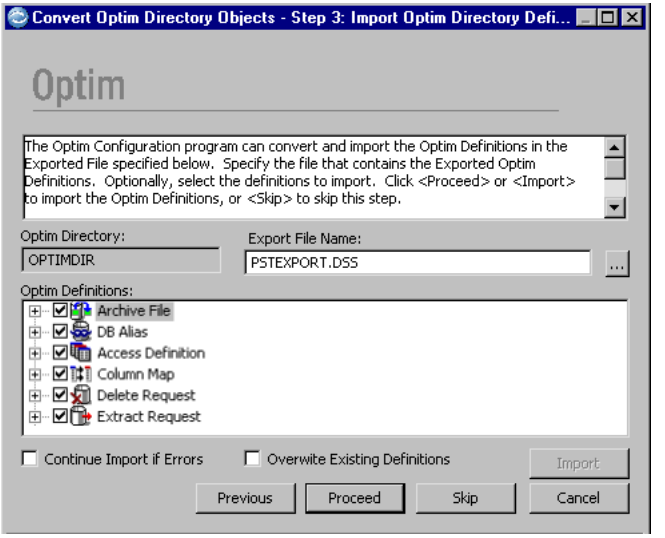


Connection String The name or string needed for the server to access the ***Optim*** Directory database.

Password Enter the password (up to 30 characters) that corresponds to the specified User ID.

Import Optim Directory Definitions

After the workstation is connected to the database, you can import the objects using the **Import Optim Directory Definitions** dialog.


Convert Optim Directory Objects - Step 3: Import Optim Directory Defi...
Optim
The Optim Configuration program can convert and import the Optim Definitions in the Exported File specified below. Specify the file that contains the Exported Optim Definitions. Optionally, select the definitions to import. Click <Proceed> or <Import> to import the Optim Definitions, or <Skip> to skip this step.
Optim Directory:
OPTIMDIR
Export File Name:
PSTEXPORT.DSS
Optim Definitions:
Archive File
DB Alias
Access Definition
Column Map
Delete Request
Extract Request
Continue Import if Errors
Overwite Existing Definitions
Import
Previous
Proceed
Skip
Cancel

Optim Directory

Name of the ***Optim*** Directory into which objects are imported.

Export File Name

Enter the name of the Export File. The Export File was created during the Export Process and contains the object definitions to import.

Optim Definitions

Identifies the objects in the Export File. You can display a list of objects of a certain type by clicking the plus (+) sign. Select the check boxes associated with the objects you want to import. To exclude an object, clear the corresponding check box. You must select at least one object definition to run the Import Process.

Continue Import if Errors

Indicate whether processing should stop if an error occurs. To continue processing if an error occurs, select the check box. To halt processing if an error occurs, clear the check box.

Overwrite Existing Definitions

Indicate what action is required when the name of an imported object matches that of an object already in the current ***Optim*** Directory:

- To select any or all objects and overwrite the existing definitions in the Directory, select the check box.
- To prevent overwriting objects, clear the check box.

Run Import

There are two ways to run the Import Process:

- If you want to import all selected objects at one time (i.e., in one import process), click **Next**.
- If you want to import a group of objects in one import process, and import another group in a separate import process, click **Import**. Each time you click **Import**, the objects selected in the **Optim Definitions** list are processed, but the Import dialog remains displayed so you can select the next group of objects you want to import.

  For example, if you want to import all Access Definitions in one import process, import all Table Maps in another import process, and import all Calendars in a third import process, do the following:

  1. Select the Access Definitions you want to import in the **Optim Definitions** list, and then click **Import**.
  2. After the selected Access Definitions are processed, select the Table Maps you want to import, and click **Import** again.
  3. After the selected Table Maps are processed, select the Calendars you want to import, and click **Import** a third time. (Alternatively, you can click **Next** when you are ready to process the last group of objects you want to import, as discussed in the ***Note*** following step 4.)
  4. When you are done importing objects, click **Skip** to display the **Complete** dialog, described under **Conversion Complete** on page 582.

     Note: When you are ready to process the last group of objects you want to import, you can click **Next**, instead of **Import**, to complete the import process. If you do that, you do not have to click **Skip** to display the **Complete** dialog.

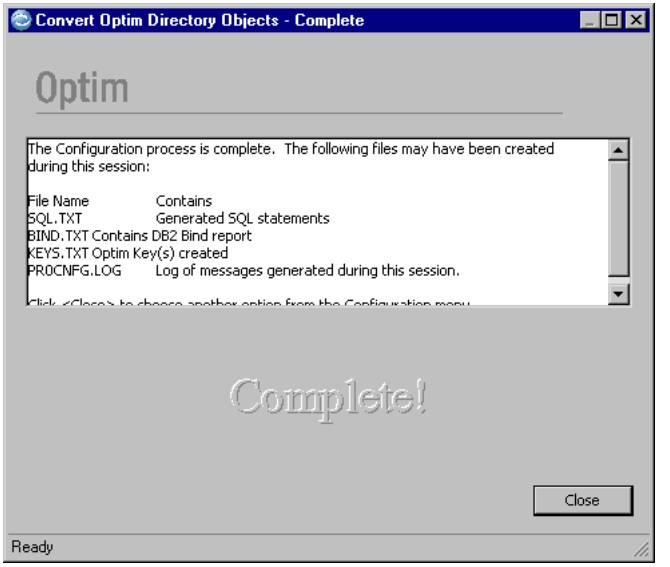
During import processing, the status bar displays information about the import process. After processing completes, imported objects are identified by a gray check box.

If any errors occur, processing continues or stops based on the setting specified for the **Continue Import if Errors** prompt. Errors are identified by a red "X" beside each object in error. If the **Overwrite**

Existing Definitions check box is cleared, duplicate definitions are noted in bold, and they are not imported. If some objects fail to be imported due to errors, check the specifications, and then retry the import process by clicking **Import**.

Conversion Complete

When you are finish importing objects, the Conversion Process opens the **Complete** dialog. Click **Close** on that dialog to return to the Configuration main window, where you can quit the program or perform other tasks.


Convert Optim Directory Objects - Complete
Optim
The Configuration process is complete. The following files may have been created during this session:
File Name Contains
SQL.TXT Generated SQL statements
BIND.TXT Contains DB2 Bind report
KEYS.TXT Optim Key(s) created
PROCNFG.LOG Log of messages generated during this session.
Complete!
Close
Ready

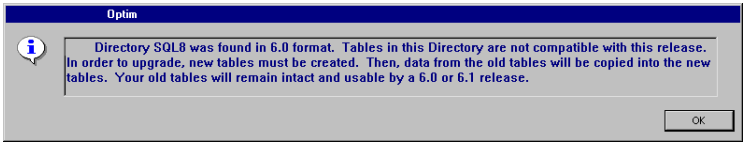
G.2 Conversion Process for Directory Tables on SQL Server

The Conversion Process for a version 6.0/6.1 ***Optim*** Directory on an SQL Server database is part of the normal Directory maintenance performed after installing a new version of ***Optim***. After performing the conversion, you can keep or drop the old Directory.

G.2.1 Converting Version 6.0/6.1 Directory Tables in SQL Server

To convert version 6.0/6.1 ***Optim*** Directory tables in an SQL Server database, use the **Create/Update Optim Directory** or **Apply Maintenance for Optim Directory Access** options available from the **Configuration** program **Tasks** menu.

After selecting an ***Optim*** Directory and completing the **Connect to Database** dialog (see page 569), a pop-up warns you that new Directory tables will be created and the old tables will still be available to your 6.0/6.1 release.


Optim
Directory SQL8 was found in 6.0 format. Tables in this Directory are not compatible with this release. In order to upgrade, new tables must be created. Then, data from the old tables will be copied into the new tables. Your old tables will remain intact and usable by a 6.0 or 6.1 release.
OK

Click **OK** to continue the Conversion Process and open the **Update Directory Tables** dialog. Click **Proceed** to create the 6.2 ***Optim*** Directory tables and continue the **Configuration** program task.

G.2.2 Dropping Version 6.0/6.1 Directory Tables

After an ***Optim*** Directory in an SQL Server database has been converted, you can drop the version 6.0/6.1 Directory tables. To drop the 6.0/6.1 Directory tables, select **Drop DB Alias or Optim Tables** from the **Configuration** program **Tasks** menu.

Specify Optim Directory

Use the **Specify Optim Directory** dialog to select the name of the version 6.0/6.1 ***Optim*** Directory you want to drop. Click **Proceed** to continue.

Connect to Database

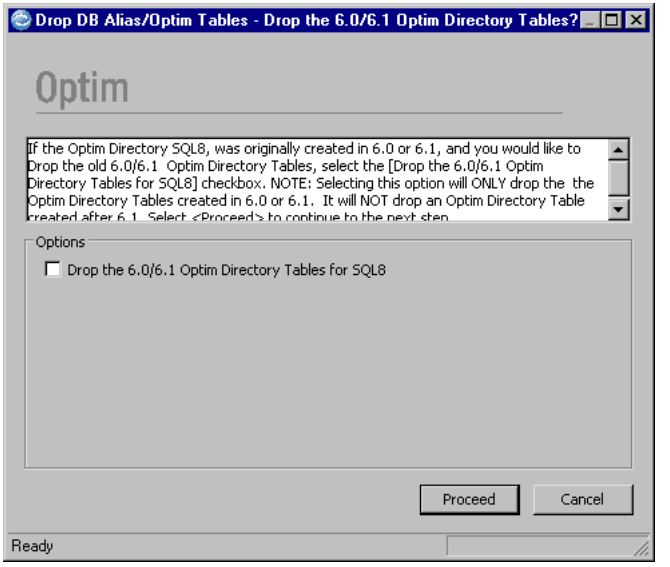
The **Configuration** program must connect to the database to drop the ***Optim*** Directory tables. Use the **Connect to Database** dialog to provide the connection information. Click **Proceed** to continue.

Create/Select DB Alias

In the **Create/Select DB Alias** dialog, click **Skip** to continue the process of dropping the version 6.0/6.1 tables. Do not click **Proceed**, or the **Configuration** program will drop the DB Alias for your new ***Optim*** Directory.

Drop the 6.0/6.1 Optim Directory Tables?

In the **Drop the 6.0/6.1 Optim Directory Tables?** dialog, select **Drop the 6.0/6.1 Optim Directory Tables** to make the Directory unavailable to the ***Optim*** products version 6.0/6.1. Click **Proceed** to continue.


Drop DB Alias/Optim Tables - Drop the 6.0/6.1 Optim Directory Tables?
Optim
If the Optim Directory SQL8, was originally created in 6.0 or 6.1, and you would like to Drop the old 6.0/6.1 Optim Directory Tables, select the [Drop the 6.0/6.1 Optim Directory Tables for SQL8] checkbox. NOTE: Selecting this option will ONLY drop the the Optim Directory Tables created in 6.0 or 6.1. It will NOT drop an Optim Directory Table
Options
Drop the 6.0/6.1 Optim Directory Tables for SQL8
Proceed
Cancel
Ready

Connect to Database

The **Configuration** program must re-connect to the database to drop the ***Optim*** Directory tables. Use the **Connect to Database** dialog to provide the connection information. Click **Proceed** to continue.

Drop Optim Directory Tables

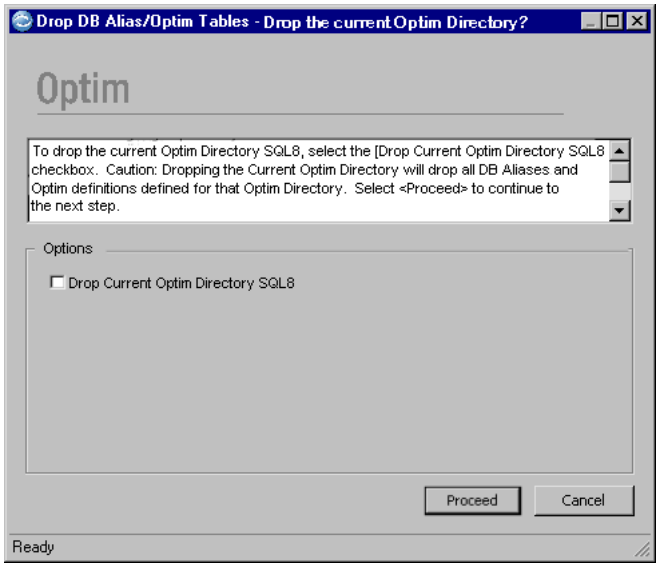
Before you drop an ***Optim*** Directory (and ***Optim*** Directory tables), the **Configuration** program displays the table identifier and prompts you to review the generated SQL, using the **Drop Directory Tables** dialog. Click **Proceed** to drop the 6.0/6.1 Directory tables and continue.

Create/Drop Stored Procedures

Use the **Create/Drop Stored Procedures** dialog to drop the stored procedures SQL Server uses to access tables in the 6.0/6.1 Directory. Click **Proceed** to continue.

Drop the Current Directory?

In the **Drop the Current Directory?** dialog, select **Drop Current Directory** to drop all DB Aliases and object definitions in the 6.0/6.1 Directory. Click **Proceed** to continue.


Drop DB Alias/Optim Tables - Drop the current Optim Directory?
Optim
To drop the current Optim Directory SQL8, select the [Drop Current Optim Directory SQL8 checkbox. Caution: Dropping the Current Optim Directory will drop all DB Aliases and Optim definitions defined for that Optim Directory. Select <Proceed> to continue to the next step.
Options
Drop Current Optim Directory SQL8
Proceed
Cancel
Ready

Connect to Database

The **Configuration** program must connect to the database in order to drop the DB Aliases, object definitions, and stored procedures. Use the **Connect to Database** dialog to provide the connection information for the Directory. Click **Proceed** to continue.

Appendix H. Samples

The installation CD provides sample data and files to be used with ***Optim***. Sample database tables are not generally loaded until configuration but, when you install ***Optim***, you can choose to install sample files. (For more information, see **Sample Files** on page 43.) If you install the sample files, the installation creates a subdirectory entitled Samples in the ...\IBM Optim\RT subdirectory.

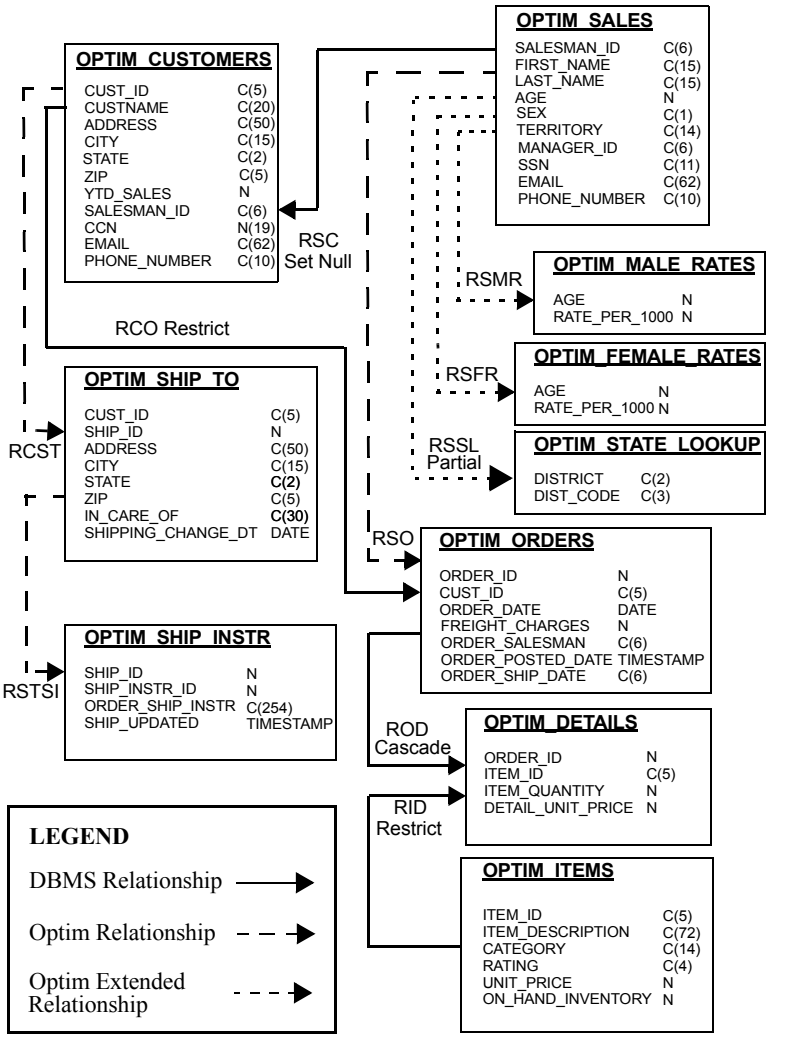
The Samples subdirectory contains the following:

CMExit	Contains sample exit routines for Column Maps.
CMProc	Contains files for creating sample Column Map procedures.
Extract	Contains sample Extract Files.
JCL	Contains the sample JCL file.

Both the ***Optim*** sample database and the samples in the Samples subdirectory are described in this Appendix.

H.1 Sample Database Tables and Structure

Sample database tables and data are distributed on the installation CD and are loaded during the configuration process. (Refer to **Load Sample Tables** on page 112.) As a group, the database tables include information on customers and orders, with shipping instructions. The sample tables also include information about sales and inventory. Minor differences in data types exist, depending upon the DBMS you use to install the sample tables. The following diagram shows the basic structure of the sample database.



This diagram shows the relationships among the tables, as follows:

- Arrows indicate the flow from parent to child.
- Solid lines represent relationships defined to the DBMS.
- Dashed lines indicate relationships defined to the ***Optim*** Directory during training and demonstrations.
- Dotted lines indicate ***Optim*** Extended Relationships. Extended relationships can emulate implicit, or application-managed, relationships in your database, allowing you to manipulate sets of relational data in the same manner as in your production environment.
- Data is provided for all tables in the sample database shown in the diagram.

An additional set of tables is also installed with the sample database. Tables in the additional set have the same names as tables in the first set, with the suffix "2" appended. The four tables in this additional set are:

- OPTIM_CUSTOMERS2
- OPTIM_ORDERS2
- OPTIM_DETAILS2
- OPTIM_ITEMS2

Tables in the additional set do not contain data. They are used to demonstrate the facilities in ***Optim***.

H.1.1 OPTIM_SALES Table

The OPTIM_SALES table identifies each salesperson by name, ID number and manager. The OPTIM_SALES table has the following columns:

Column Name	Data Type and Description
SALESMAN_ID	CHAR; up to 6 characters; cannot contain null.
FIRST_NAME	CHAR; up to 15 characters; cannot contain null.
LAST_NAME	CHAR; up to 15 characters; cannot contain null.
AGE	INTEGER; cannot contain null; has a default value.
SEX	CHAR; 1 character; cannot contain null; has a default value.
TERRITORY	VARCHAR; up to 14 characters; cannot contain null.
MANAGER_ID	CHAR; up to 6 characters.
SSN	CHAR; up to 11 characters; cannot contain null.
EMAIL	VARCHAR2; up to 62 characters; cannot contain null.
PHONE_NUMBER	CHAR; up to 10 characters; can contain a null value.

Primary Keys

The SALESMAN_ID column is the primary key column.

Relationships to other tables

The OPTIM_SALES table is a parent of:

- The OPTIM_CUSTOMERS table, through a foreign key on column SALESMAN_ID.
- The OPTIM_MALE_RATES table, through an ***Optim*** data-driven relationship on column AGE when SEX = ‘M’.

- The OPTIM_FEMALE_RATES table, through an ***Optim*** data-driven relationship on column AGE when SEX = ‘F’.
- The OPTIM_STATE_LOOKUP table, through an ***Optim*** substring relationship using SUBSTR(SALESMAN_ID,1,2).

H.1.2 OPTIM_CUSTOMERS Table

The OPTIM_CUSTOMERS table contains customer names, ID numbers, and addresses. The OPTIM_CUSTOMERS table has the following columns:

Column Name	Data Type and Description
CUST_ID	CHAR; up to 5 characters; cannot contain null; contains a check constraint.
CUSTNAME	CHAR; up to 20 characters; cannot contain null.
ADDRESS	VARCHAR; up to 50 characters; cannot contain null.
CITY	VARCHAR; up to 15 characters; cannot contain null.
STATE	CHAR; up to 2 characters; cannot contain null.
ZIP	CHAR; up to 5 characters; can contain a null value.
YTD_SALES	DECIMAL; dollar amount; cannot contain null; has a default value.
SALESMAN_ID	CHAR; up to 6 characters; can contain a null value.
CCN	INTEGER; 19 characters; cannot contain null.
EMAIL	VARCHAR2; up to 62 characters; cannot contain null.
PHONE_NUMBER	CHAR; up to 10 characters; can contain a null value.

Primary Keys

The CUST_ID column is the primary key column.

Relationships to other tables

The OPTIM_CUSTOMERS table is a parent of:

- The OPTIM_ORDERS table, through a foreign key on column CUST_ID.
- The OPTIM_SHIP_TO table, through an ***Optim*** relationship on column CUST_ID.

The OPTIM_CUSTOMERS table is a child of:

- The OPTIM_SALES table, through its foreign key on column SALESMAN_ID.

H.1.3 OPTIM_ORDERS Table

The OPTIM_ORDERS table contains information for orders, including order number, customer ID, and salesman. The OPTIM_ORDERS table has the following columns:

Column Name	Data Type and Description
ORDER_ID	DECIMAL; order ID number; cannot contain null.
CUST_ID	CHAR; customer ID number; up to 5 characters; cannot contain null.
ORDER_DATE	DATE; date of order; cannot contain null; has default value.
ORDER_TIME	TIME; time of day; cannot contain null; has default value.
FREIGHT_CHARGES	DECIMAL; dollar amount; can contain null value.
ORDER_SALESMAN	CHAR; up to 6 characters; can contain null value.
ORDER_POSTED_DATE	TIMESTAMP; cannot contain null; has default value.
ORDER_SHIP_DATE	CHAR; date when order is shipped; up to 8 characters; cannot contain null; has default value.

Primary Keys

The ORDER_ID column is the primary key column.

Relationships to other tables

The OPTIM_ORDERS table is a parent of the OPTIM_DETAILS table, through a foreign key on column ORDER_ID.

The OPTIM_ORDERS table is a child of the OPTIM_CUSTOMERS table, through its foreign key on column CUST_ID.

H.1.4 OPTIM_DETAILS Table

The OPTIM_DETAILS table contains additional information for each order in the OPTIM_ORDERS table. The OPTIM_DETAILS table has the following columns:

Column Name	Description and Data Type
ORDER_ID	DECIMAL; order ID number; cannot contain null.
ITEM_ID	CHAR; item ID number; cannot contain null.
ITEM_QUANTITY	SMALLINT; number of items; cannot contain null.
DETAIL_UNIT_PRICE	DECIMAL; unit price; dollar amount; cannot contain null.

Primary Keys

The ORDER_ID and ITEM_ID columns are the primary key.

Relationships to other tables

The OPTIM_DETAILS table is a child of:

- The OPTIM_ORDERS table, through its foreign key on column ORDER_ID.
- The OPTIM_ITEMS table, through its foreign key on column ITEM_ID.

H.1.5 OPTIM_ITEMS Table

The OPTIM_ITEMS table contains information about each item for an order, including description, price, and quantity in inventory. The OPTIM_ITEMS table has the following columns:

Column Name	Description and Data Type
ITEM_ID	CHAR; up to 5 characters; cannot contain null.
ITEM_DESCRIPTION	VARCHAR; up to 72 characters; cannot contain null.
CATEGORY	VARCHAR; up to 14 characters; cannot contain null.
RATING	CHAR; up to 4 characters; cannot contain null.
UNIT_PRICE	DECIMAL; dollar amount; cannot contain null.
ON_HAND_INVENTORY	INTEGER; cannot contain null.

Primary Keys

The ITEM_ID column is the primary key column.

Relationships to other tables

The OPTIM_ITEMS table is a parent of the OPTIM_DETAILS table, through a foreign key on column ITEM_ID.

H.1.6 OPTIM_SHIP_TO Table

The OPTIM_SHIP_TO table contains order shipping information. The OPTIM_SHIP_TO table has the following columns:

Column Name	Data Type and Description
CUST_ID	CHAR; up to 5 characters; cannot contain null.
SHIP_ID	SMALLINT; cannot contain null.
ADDRESS	VARCHAR; up to 50 characters; can contain a null value.
CITY	VARCHAR; up to 15 characters; can contain a null value.
STATE	CHAR; 2 character abbreviation; can contain a null value.
ZIP	DECIMAL; can contain a null value.
IN_CARE_OF	VARCHAR; up to 30 characters; can contain a null value.
SHIPPING_CHANGE_DT	DATE; cannot contains nulls; has default value.

Primary Keys

The SHIP_ID column is the primary key column.

Relationships to other tables

The OPTIM_SHIP_TO table is a parent of the OPTIM_SHIP_INSTR table, through an ***Optim*** relationship on column SHIP_ID.

The OPTIM_SHIP_TO table is a child of the OPTIM_CUSTOMERS table, through its ***Optim*** relationship on column CUST_ID.

H.1.7 OPTIM_SHIP_ INSTR Table

The OPTIM_SHIP_INSTR table contains detailed information for order shipping. The OPTIM_SHIP_INSTR table has the following columns:

Column Name	Data Type and Description
SHIP_ID	SMALLINT; can contain a null value.
SHIP_INSTR_ID	DECIMAL; can contain a null value.
ORDER_SHIP_INSTR	VARCHAR; up to 254 characters; default value “FEDERAL EXPRESS”.
SHIP_UPDATED	TIMESTAMP; cannot contain null; has default value.

Primary Keys The SHIP_INSTR_ID column is the primary key column.

Relationships to other tables The OPTIM_SHIP_INSTR table is a child of the OPTIM_SHIP_TO table, through its ***Optim*** relationship on column SHIP_ID.

H.1.8 OPTIM_MALE_RATES Table

The OPTIM_MALE_RATES table contains insurance rates, based on age. The OPTIM_MALE_RATES table has the following columns:

Column Name	Data Type and Description
AGE	INTEGER; can contain a null value.
RATE_PER_1000	DECIMAL; rate in dollar amount; can contain a null value.

Primary Keys The RATE_PER_1000 column is the primary key column.

Relationships to other tables The OPTIM_MALE_RATES table is a child of the OPTIM_SALES table, through its ***Optim*** data-driven relationship on column AGE.

H.1.9 OPTIM_FEMALE_RATES Table

The OPTIM_FEMALE_RATES table contains insurance rates based on age. The OPTIM_FEMALE_RATES table has the following columns:

Column Name	Data Type and Description
AGE	INTEGER; can contain a null value.
RATE_PER_1000	DECIMAL; rate in dollar amount; can contain a null value.

Primary Keys

The RATE_PER_1000 column is the primary key column.

Relationships to other tables

The OPTIM_FEMALE_RATES table is a child of the OPTIM_SALES table, through its ***Optim*** data-driven relationship on column AGE.

H.1.10 OPTIM_STATE_LOOKUP Table

The OPTIM_STATE_LOOKUP table has the following columns:

Column Name	Data Type and Description
DIST_CODE	CHAR; 3 characters; cannot contain a null value.
DISTRICT	CHAR; 2 characters; cannot contain a null value.

Primary Keys

The OPTIM_STATE_LOOKUP table does not have a primary key.

Relationships to other tables

The OPTIM_STATE_LOOKUP table is a child of the OPTIM_SALES table through a substring relationship on column DISTRICT using SUBSTR(SALESMAN_ID,1,2).

H.2 Sample Column Map Exits

The \Samples\CMExit subdirectory includes a set of sample exit routines. These commented samples show how to use the data areas available for exit routines and provide examples of the type of processing that can be performed using an exit.

Note: Column Map Exits must be compiled and linked, and must conform to C programming language calling conventions.

Sample exit routines included are:

PSTEXIT.C	Samples of the three types of exit routines - standard, source format, and destination format.
PSTEXIT.dll	Compiled versions of the three sample exit routines.
PSTEXIT.h **PSTCMEXIT.h**	Required header files.
PSTEXIT.mak	A sample make file.

Note: For complete information about Column Map Exits, refer to the **Common Elements Manual,** **Appendix B. Exit Routines for Column Maps**.

Sample Standard Exit

A **Standard Exit** routine is called to derive the value for a destination column in a Column Map. This sample performs two operations on the sample database table OPTIM_CUSTOMERS, as follows:

- Discards rows that have a value of zero (0) in the YTD_SALES column, and processes all other rows.
- Assigns a value of ‘SE003 ’ to the SALESMAN_ID column for all customers in Florida (rows with FL in the STATE column).

To reference this sample in a Column Map, you must specify **EXIT PSTEXIT** in the source column for the destination column SALESMAN_ID.

Sample Source Format Exit

A **Source Format Exit** is typically called to format the source column, for example, for an Age Function that otherwise would not be supported in a Column Map.

The sample performs the following operations on the sample database table OPTIM_ORDERS:

- Discards rows that have a value of ‘SE012’ in the SALESMAN_ID column, and processes all other rows.
- Ages ORDER_DATE for rows that have a value of ‘SE0005’ in the SALESMAN_ID column, and skips all other rows.

To use this sample, you must specify the exit routine as part of the Age Function in the ORDER_DATE source column of the Column Map as follows:

AGE(+1W,SC=ORDER_DATE,SRCEXIT=PSTEXIT)

Sample Destination Format Exit

A **Destination Format Exit** is typically called to format the destination column, for example, for an Age Function that otherwise would not be supported in a Column Map.

The sample performs the following operations on the sample database table OPTIM_ORDERS:

- Discards rows that have a value of ‘SE012’ in the SALESMAN_ID column, and processes all other rows.
- Ages ORDER_SHIP_DATE for rows that have a value of ‘SE0005’ in the SALESMAN_ID column, and skips all other rows.

To use this sample, you must specify the exit routine as part of the Age Function in the ORDER_SHIP_DATE source column of the Column Map as follows:

AGE(1W,SC=ORDER_SHIP_DATE,SF='YY/MM/DD', DSTEXIT=PSTEXIT)

H.3 Sample Column Map Procedures

A Column Map Procedure is a custom program written in ***Optim Basic*** that is referenced to perform special processing or data manipulation that is otherwise beyond the scope of a Column Map.

The function of a Column Map Procedure is generally the same as that of an exit routine. Exit routines, however, are written outside ***Optim*** and must be externally compiled and linked. Column Map Procedures are written within ***Optim***.

The \Samples\CMProc subdirectory includes sample files written in ***Optim Basic*** that can be used to create a set of Column Map procedures. The file names are:

CMEXIT.BAS Sample ***Optim Basic*** Column Map procedure modeled after the Standard Exit routine. Refer to **Sample Standard Exit**.

TBLINFO.BAS Sample ***Optim Basic*** Column Map procedure that demonstrates how to access and retrieve data about the process, product or database table. This sample procedure moves source data to the destination without changing it, and can be used with most column data types.

DEFAULT.BAS Sample ***Optim Basic*** Column Map procedure used to populate the Column Map Procedure Editor when installed in the BIN subdirectory.

To create a Column Map Procedure from one of the files provided:

1. In the main window, select **Column Map Proc** from the **Definitions** menu to open the **Column Map Proc Editor** and last edited Column Map Proc.
2. Select **New** from the **File** menu in the **Column Map Proc Editor**.
3. Select **Import** from the **File** menu in the **Column Map Proc Editor** to open the **Supply an Import File Name** dialog.
4. Type (or click the Browse button and select) the path to the Samples subdirectory containing the sample files, and the file name: (e.g., C:\Program Files\IBM Optim\RT\Samples\CMProc\CMEXIT.BAS)

5. Select **Save As** from the **File** menu in the **Column Map Proc Editor**. In the **Save a Column Map Proc** dialog, type a name in the Pattern box and click Save.
6. Edit the Column Map Proc, as needed.
7. Compile.

Sample Standard Procedure

A **Standard** procedure is called to derive the value for a destination column in a Column Map. This sample Column Map procedure is created from the CMExit.bas file provided, as described above. This procedure performs two operations on the sample database table OPTIM_CUSTOMERS, as follows:

- Discards rows that have a value of zero (0) in the YTD_SALES column, and processes all other rows.
- Assigns a value of 'SE012' to the SALESMAN_ID column for customers in Florida (rows with FL in the STATE column).

To use this sample in a Column Map, you must specify **PROC CMEXIT.BAS** in the source column for the destination column SALESMAN_ID.

Sample Table Information Procedure

The sample table information Column Map procedure is created from the TBLINFO.BAS file as described above. This sample is provided to demonstrate the ***Optim Basic*** Column Map procedures that you can use to retrieve data about a process, product or database table. This procedure moves unchanged source data to the destination, and demonstrates how to output the following:

- Name of ***Optim*** Temp Directory
- Name of ***Optim*** Data Directory
- Name of ***Optim*** Script
- Company Name
- ***Optim*** Release Number
- ***Optim*** Build Number
- ***Optim*** Error Codes
- Instance
- Thread ID
- Thread Handle
- Operating System
- Operating System Release

- Operating System Build
- Operating System Service Pack
- Server User ID
- Computer Name

H.4 Sample Extract Files

The following Extract Files are included in the Samples\Extract subdirectory:

CSB4DATA.XF PSTDEMO.XF	These Extract Files contain data from the sample database that has been altered slightly. These files are useful for training or learning about features of ***Compare***.
PSTD_IFX.XF PSTD_MSS.XF PSTD_MVS.XF PSTD_ORA.XF PSTD_SYB.XF PSTD_UDB.XF	These Extract Files duplicate the data in PSTDEMO.XF in DBMS-specific format.
SAMP_390.XF SAMP_DB2.XF SAMP_IFX.XF SAMP_MSS.XF SAMP_MVS.XF SAMP_ORC.XF SAMP_SYB.XF	These Extract Files provide DBMS-specific copies of the ***Optim*** sample database data.

H.5 Sample JCL File

The sample JCL file (LOADDB2.jcl) for running the DB2 z/OS loader from an ***Optim Server*** is included in the Samples\JCL subdirectory.

Appendix I. Data Privacy Data Tables

Data privacy data tables are available to clients who have an ***Optim*** Data Privacy License. These tables allow you to mask company and personal data — such as employee names, customer names, social security numbers, credit card numbers, and e-mail addresses — to generate transformed data that is both unique and valid within the context of the application. Generally, these data privacy tables are loaded when you configure the first workstation, but you also can load them independently or when you configure an additional DB Alias.

You can use the data privacy data tables to:

- Prevent internal privacy breaches by de-identifying or masking the data available to developers, quality assurance testers, and other personnel.
- Improve privacy compliance initiatives by substituting customer data with contextually accurate, but fictionalized data.
- Protect confidential customer information and employee data in your application development and testing environments.
- Ensure valid test results by propagating masked elements across related tables to ensure the referential integrity of the database.

If you have an ***Optim*** Data Privacy License, the data privacy data tables are available on the installation CD in a *privacy.xf* extract file that is loaded during the configuration process. (See **Load/Drop Data Privacy Tables** on page 115.)

I.1 Content of Data Privacy Tables

The Privacy Extract file, *privacy.xf,* includes the tables described in this section. The tables include lookup information on companies and individuals that can be used for data masking or data privacy processing. Minor differences in data types exist, depending upon the DBMS you use to install the data privacy tables.

PERSON Table

The PERSON table contains the following columns and data:

Column Name	Data Type and Description
EMPNO	Employee number. CHAR; 6 characters.
NATIONAL_ID	National ID, such as a social security number (SSN). CHAR; 20 characters.
NATIONAL_ID_TYPE	National ID type, such as USSSN for US Social Security Number. CHAR; 6 characters.
ADDR_STREET1	First line of street address. VARCHAR; 30 characters.
ADDR_STREET2	Second line of street address. VARCHAR; 30 characters.
ADDR_CITY	City. CHAR; 20 characters.
ADDR_STATE	State abbreviation. CHAR; 6 characters.
ADDR_ZIP	ZIP code. CHAR; 6 characters.
ADDR_COUNTRY	Country abbreviation. CHAR; 3 characters.
PHONE_NUMBER	Phone number, including area code. CHAR; 20 characters.

PHONE_COUNTRY	Country code for international calls. CHAR; 20 characters.
SALARY	Person's salary. DECIMAL; 11 places with 2 decimal places.
NAME_FIRST	First name. CHAR; 15 characters.
NAME_INITIAL	Middle initial. CHAR; 1 character.
NAME_LAST	Last name. CHAR; 15 characters.
NAME_FULL	Full name: first name, middle initial, and last name. VARCHAR; 40 characters.
BIRTHDATE	Birth date. DATE.
GENDER	M = Male, F = Female. CHAR; 1 character.
EMAIL	Email address. CHAR; 70 characters.
CREDITCARD	Credit card number. CHAR; 19 characters.

ADDRESS Table

The ADDRESS table contains the following columns and data:

Column Name	Data Type and Description
SEQ	Unique, sequential number. INTEGER.
ADDRESS	Street address. CHAR; 50 characters.
CITY	City. CHAR; 28 characters.
STATE	State abbreviation. CHAR; 2 characters.
ZIPCODE	ZIP code. CHAR; 5 characters.
ZIPPLUS4	Extended portion of US ZIP code. CHAR; 4 characters.

Note: Data in the ADDRESS table is copyrighted by the United States Postal Service and is provided with permission.

COMPANY Table

The COMPANY table has the following columns and data:

Column Name	Data Type and Description
SEQ	Unique, sequential number. INTEGER.
DATAVALUE	Company name. CHAR; 40 characters.

Note: Data in the COMPANY table is copyrighted by the United States Postal Service and is provided with permission.

FIRSTNAME Table

The FIRSTNAME table has the following columns and data:

Column Name	Data Type and Description
SEQ	Unique, sequential number. INTEGER.
DATAVALUE	First name. CHAR; 15 characters.

FIRSTNAME_F Table

The FIRSTNAME_F table has the following columns and data for females:

Column Name	Data Type and Description
SEQ	Unique, sequential number. INTEGER.
DATAVALUE	First name. CHAR; 15 characters.

FIRSTNAME_M Table

The FIRSTNAME_M table has the following columns and data for males:

Column Name	Data Type and Description
SEQ	Unique, sequential number. INTEGER.
DATAVALUE	First name. CHAR; 15 characters.

LASTNAME Table

The LASTNAME table has the following columns and data:

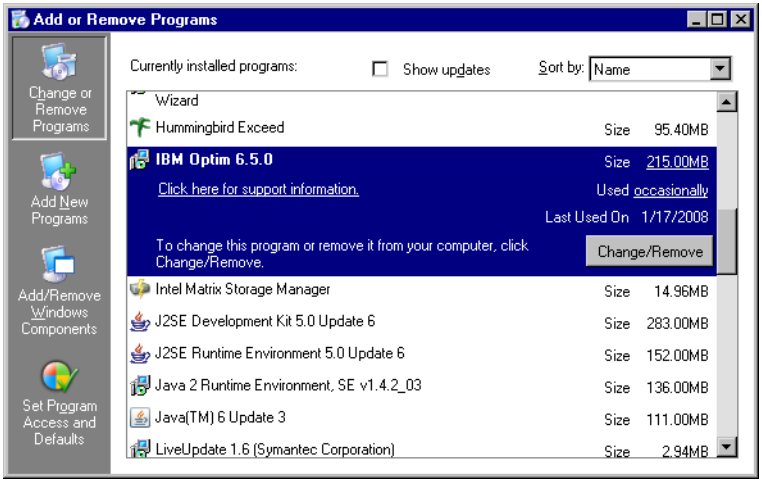
Column Name	Data Type and Description
SEQ	Unique, sequential number. INTEGER.
DATAVALUE	Last name. CHAR; 15 characters.

Appendix J. Uninstalling

To remove ***Optim*** from a workstation, use the **Add/Remove Programs** utility in the Windows Control Panel, as follows.

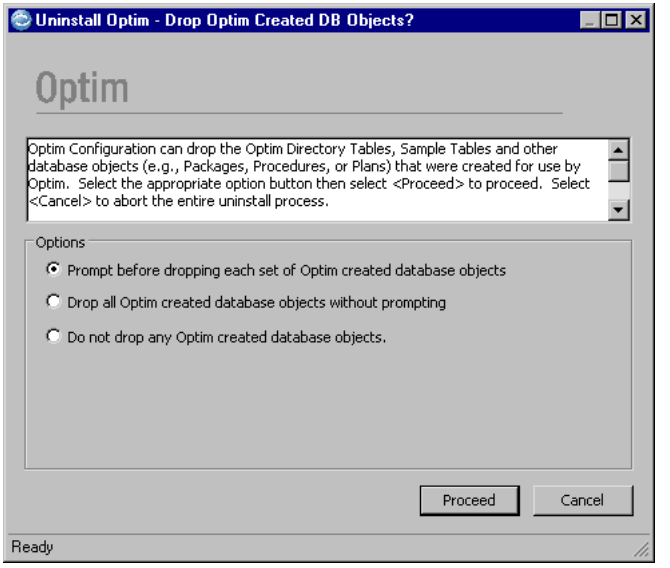
Select **Add/Remove Programs** from the Windows Control Panel.

Select **IBM Optim** from the list of programs on the **Add/Remove Programs** dialog.



Click **Change/Remove** to run the **Configuration** program.

The **Uninstall Optim - Drop Optim Created DB Objects** dialog is displayed.


Uninstall Optim - Drop Optim Created DB Objects?
Optim
Optim Configuration can drop the Optim Directory Tables, Sample Tables and other database objects (e.g., Packages, Procedures, or Plans) that were created for use by Optim. Select the appropriate option button then select <Proceed> to proceed. Select <Cancel> to abort the entire uninstall process.
Options
Prompt before dropping each set of Optim created database objects
Drop all Optim created database objects without prompting
Do not drop any Optim created database objects.
Proceed
Cancel
Ready

Select one of the three options:

- Prompt before dropping each set of ***Optim*** created database objects.
- Drop all ***Optim*** created database objects without prompting.
- Do not drop any ***Optim*** created database objects.

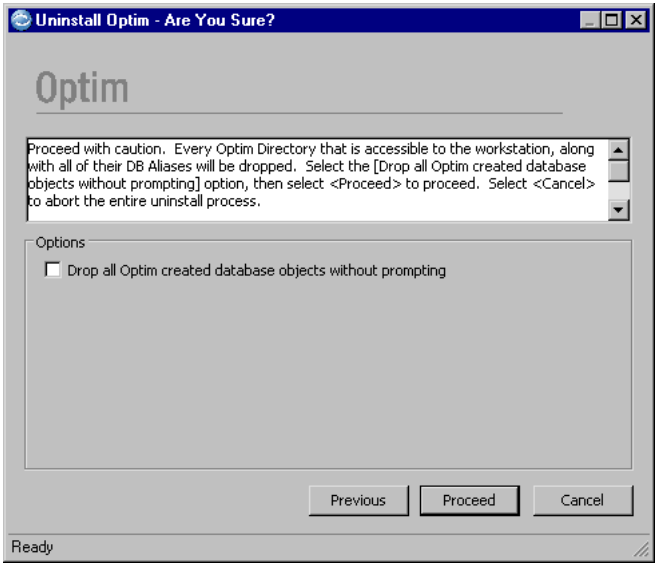
J.1 Prompt Before Dropping Each Set of Optim Database Objects

When you select this option, and click **Proceed**, you are prompted to confirm the deletion of each object. After all objects have been dropped, you are asked to confirm deletion of the ***Optim*** Archive ODBC Interface driver.

Refer to **7.17 Drop DB Alias or Optim Tables** on page 238 for the sequence in which you are asked to confirm the deletion of ***Optim*** created database objects.

J.2 Drop All Optim Created Database Objects Without Prompting

When you select this option, and click **Proceed**, you are cautioned that every ***Optim*** Directory and DB Alias accessible from the workstation will be dropped without further prompting.


Uninstall Optim - Are You Sure?
Optim
Proceed with caution. Every Optim Directory that is accessible to the workstation, along with all of their DB Aliases will be dropped. Select the [Drop all Optim created database objects without prompting] option, then select <Proceed> to proceed. Select <Cancel> to abort the entire uninstall process.
Options
Drop all Optim created database objects without prompting
Previous
Proceed
Cancel
Ready

Select the check box on the **Are You Sure** dialog and click **Proceed** to drop all ***Optim*** objects. Click **Cancel** to abort the uninstall process.

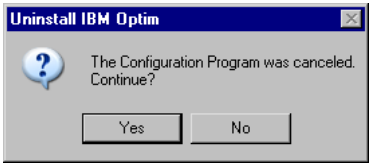
If a password is required to access a particular database, you will be prompted for it. When the ***Optim*** sample database tables are to be dropped, you will be prompted to confirm that the correct tables are dropped. When the data privacy tables are to be dropped, you will also be prompted to confirm that the correct tables are dropped.

J.3 Do Not Drop Any Optim Created Database Objects

When you select this option, and click **Proceed**, all ***Optim*** created database objects remain unchanged and intact, but the ***Optim*** software is removed from the workstation.

J.4 Cancel the Uninstall Process

If you select **Cancel** on any window, the **Configuration** program exits and a confirmation is displayed.



- Click **Yes** to close the confirmation dialog and continue the uninstall process.
- Click **No** to cancel the uninstall process.

Index

A

Access Control Domain
- definition ... 444
- editor ... 450
- list ... 447
- role specifications ... 452

Access Control List
- definition ... 444
- editor ... 469

Actions tab, Personal Options ... 319–323
- Column Map Procedure ... 319
- format numeric values ... 322
- maximum database connections ... 327
- monitor update frequency ... 322
- report retention ... 322
- show aging tabs ... 322
- show currency tab ... 322

Age Function
- destination format exit ... 600
- source format exit ... 600

Allocation Percent
- index defaults ... 298
- table defaults ... 297

Apply Maintenance
- add default tables ... 204
- all DB Aliases ... 209
- DB Alias Access ... 205
- Optim Directory Access ... 203
- query method ... 206
- specific DB Alias ... 207
- specific DBMS ... 212
- update DBMS version ... 228

Archive File Collection ... 561
- subsets ... 562

Archive tab, Personal Options ... 315–316
- Archive browse index directory ... 315
- Archive directory ... 315
- Archive index directory ... 315
- directory for Subset Extract Files ... 316
- file backup device ... 316
- trim search list ... 316
- use index to search ... 316

Archive tab, Product Options ... 270–273
- available file backup devices ... 270
- Centera options ... 271
- Centera retention period ... 271
- Tivoli options ... 271
- user can review data to be deleted ... 270
- WORM device retention period ... 272

Audit Tables dialog ... 262–264, 311–312
- Select Table to be Audited dialog ... 266
- summary ... 267

Auditing
- active status ... 260
- active/user status ... 260
- Audit Tables dialog ... 262–264, 311–312
- description of ... 267
- enable/disable for tables ... 312
- inactive status ... 260
- Personal Options tables list ... 311, 312
- Product Options, Edit tab ... 262
- PSTAUDIT ... 262, 311
- site defaults ... 262
- summary ... 267

B

Bind/Drop Plans
- creating a DB Alias 99
- creating Optim Directory 87

Browse tab, Personal Options 313–314
- auto switch 313
- display changed data 314
- display column attributes 313
- display row count 314
- maximum exclude rows 314
- side label display 313

Buffer Pool
- index defaults 299

C

Cascade Delete/Update Option 250, 328

Column Map Procedures
- sample 601

Command Line Interface 429–439
- examples 438–439
- keywords 432–437
- syntax 431
- syntax guidelines 429

Commit Frequency 252

Configuration
- browse SQL 75
- command buttons 74
- completion files 138
- dialog features 73
- display SQL 74
- main window 62
- menu commands 63
- planning for 10
- processing log 70–73
- Tasks menu 62, 77

Configuration Assistant
- additional workstations 140
- description of 71
- first workstation 72

Configuration File, Product Options 257–258
- current Configuration File name 257
- path to new Configuration File 258
- switch to new file when created 258

Configure Additional Workstations
- Configuration Assistant 140
- configure options 149
- create registry entry 143
- DBMS client software 9
- description of 6
- enable/disable
  - ODBC interface 149
  - Optim Server 148
- guidelines 140
- import registry entries 141
- process steps 9
- Product Configuration File 149
- task summary 150

Configure Application Servers
- description of 10
- process steps 9

Configure First Workstation
- completion files 138
- Configuration Assistant 72
- configure options 132
- create
  - DB Alias 94
  - Multiple DB Aliases 118–127
  - Optim Directory 79
  - Optim Directory tables 83
- create/drop packages
  - for DB Alias 99
  - for Optim Directory 85
- DBMS
  - for DB Alias 97
  - for Optim Directory 80
- description of 6
- export registry data 137
- load/drop sample tables 112, 114, 237
- Optim Security 128–131
- process steps 6
- product license key 78
- set personal options 136
- set product options 135
- share connection information 102
- task summary 139

Configure Options
- for additional workstations 149

for first workstation 132
personal options 136
process steps 232
product options 135
Configure Security for an Optim Directory 192
Configure the Server
process steps 151
Confirm tab, Personal Options 286
before deleting 286
before losing DDLs 286
before overwriting files 286
Convert PST Directory Objects 565–582
Create
additional Optim Directory 190
copies of DB2 relationships 235
create/drop packages 85
create/drop procedures 85
create/select DB Alias 96
primary keys 233
registry entry 143
Create tab, Personal Options 294–303
compile error drop 295
DB Alias 295
DB2 OS/390 current rules 296
Limits 296
Object Name Highlighting 296
replace UDTs 296
set alias defaults 300
set index defaults 297
set synonym defaults 302
set table defaults 296
set trigger defaults 301
Credentials 417–427
DBMS logon credentials 425–427
DB Alias access 425
maintaining 426
Optim Directory access 425
Server credentials 418–424
Linux file access 424
Oracle OS Authentication 424
registry access 423
Server privileges 422
to run processes 419
to run the Server 418
UNC network share access 422
UNIX file access 424
Customer Information Dialog 39

D

Data Privacy Tables
descriptions 606–609
loading 114, 237
Database
sample tables 588
Database Permissions 14
Database tab, Product Options 252–256
allow insert action delete option 253
allow parallel processing 255
allow user to lock tables 253
Extract using Uncommitted Read 254
maximum commit frequency 252
maximum database connections 255
Sybase unchained mode 252
DB Alias
configure first workstation 94
create 7
create/drop packages 99
create/select 96
create/update 96, 185
create/update another 117
description of 94
maintain access 205
purging 244
share connection information 102
specify DBMS for 97
DB2
bind/drop plans
for DB Alias 99
for Optim Directory 87
z/OS Buffer Pool 299
DBMS
type and version 7
Default Directories
Archive 315–316
Archive Browse Index Directory 316
Archive Index Directory 315
Data Directory 285

for DBMS loaders 293
Product Configuration File 285
scheduling 292
Temporary Work 285
Trace Files 285
Delete Processing
secured files 478
Display tab, Personal Options 287–289
column delimiters 287
Large Objects 289
main window 288
maximum fetch rows 287
maximum File menu entries 288
maximum history entries 287
menu behavior 288
null value indicator 287
system messages 289
tooltips and toolbars 288

E

Edit tab, Personal Options 308–312
audit tables 310
Audit Tables dialog 311
auditing active 310
auto switch 308
default data display 310
display column attributes 308
display deleted rows 308
display row count 310
null as default 309
prompt for variables 309
retain selection criteria 309
side label display 309
single view 309
undo levels 310
user supplies defaults 309
warn on cascade 309
Edit tab, Product Options 259–261
Audit Tables dialog 262
auditing status 260
force Browse Only 261
null as default 261
user supplies defaults 260
Email Notification 330
Errors tab, Personal Options 290–291
display lines 291
error messages font 291
hide empty message bar 291
informational messages font 290
warning messages font 291
Exit Routines
destination format exit
input to Age Function 600
samples 599
source format exit
input to Age Function 600
Export Registry Data 137
Extract Files
samples 603
Extract Uncommitted Data 254

F

File Access Definition Editor 480
File Access Definitions
using secured files 478
Functional Privileges 458

G

General tab, Personal Options 284–285
Caps mode 284
data directory 285
days to keep trace files 284
Local Optim Server (ODBC) 285
Product Configuration File 285
SQL LIKE character 284
temporary work directory 285
unchained mode 329
warn on cascade 328
z/OS code page 284
General tab, Product Options 249–251
abort Scheduler or command line 251
default calendar 250
maximum extract rows 250
maximum fetch rows 249
warn on cascade delete/update 250

I

Import Registry Data 141
Index Buffer Pools 299
Index Defaults 299
Informix
  create multiple DB Aliases 122
  create/drop procedures
    for DB Alias 99
    for Optim Directory 85
  update DBMS version 228
Initialize Optim Security 128, 147
Installation
  additional workstations 9
  first workstation 4
  Linux 335
  Optim 4
  planning for 10
  starting Setup 37
  system requirements 11
  UNIX 335
  workstations or server 5

J

JCL File
  sample 603

L

Large Objects, Personal Options 289
License Agreement 38
Linux
  command line 370–385
  commands 391–392
  customer ID 361, 372
  data directories 361
  DB Alias 375
  destination folder 339
  environment variables 386
  installation 335–357
  license agreement 338
  loader 367, 376
  locale conversion 390
  LOCALE.CONF file 390
  Optim Directory 374
  pr0pass program 399
  pstlocal configuration file 370
  pstserv configuration file 360
  RT4S shell script 389
  RTSERVER shell script 387
  RTSETENV shell script 386
  securing 394–402
    configuration files 398–402
    password file 398
  select components 341
  trace days 373
Load tab, Personal Options 293–294
  DB Alias 293
  exception tables 294
  path to DBMS Loaders 294
Load tab, Product Options 274–275
  additional loader parameters 275
  DB Alias 275
  delete when truncate fails 275
  force at run time 275
  Optim Directory 275
  override loader defaults 275
  prime new request 275
Load/Drop Data Privacy Tables 115
Load/Drop Sample Tables 112
Lock Tables 253
Logon
  for multiple DB Aliases 125
  saved for multiple DB Aliases 126
Logon tab, Personal Options 303–305
  always ask for password 305
  always fail connection 305
  connection string 305
  for Optim Directory 304
  set passwords 305
  specify User ID 304
  test database connection 305

M

Main Window
  auto size 288
  maximum components 288
Maximum

commit frequency 252
extract rows 250
fetch rows 249, 287
history lists 287
menu entries 288
visible components 288
MBCS Roundtrip Processing 255
Messages
errors 291
informational 290
limit lines to display 291
resetting 289
set font style 290
show or hide 291
warnings 291
Microsoft Debugging Utility 32
Multi-byte Support 28

N

Notify tab, Personal Options 330
Send Test eMail 182, 332

O

Object Name Highlighting 296
ODBC Interface
Enable/Disable 133, 149
Installation 42, 353
Open Data Manager (ODM) 527
Archive File Collection 561
Archive File to XML Convertor 557
Attunity Studio 534
data source 538
data type conversion 556
installation 528
JDBC Thin Client 547
ODBC Thin Client 547
runtime connection 554
secondary server 542
security 548
Optim Directory
add default tables 204
create additional 190
create tables for 83
creating 7, 79
definition of 6
export registry data 137
maintain access 203
purge registry entry 243
registry entry 7
specify DBMS 80
table identifier 7, 145
typical configuration 6
workstation access 191
Optim Exit
Prerequisities for a User-Supplied Exit 52, ... 405
Writing a User-Supplied Exit 51, 405
Optim Exit in UNIX
Invalid Credentials Specified dialog ..407
Sign Optim Exit Failed dialog ... 408–409
Signing a User-Supplied Exit 413–416
Signing an Exit during Setup 346–347
Signing Methods 406–407
Signing the default Exit after Installation 409– 412
Optim Exit in Windows
Changing a Signing Exit 55
Sign Optim Exit dialog 56–59
Signing an Exit during Configuration 53–54
Specify Company Name dialog 60
Optim Security
Access Control Domain 444, 450
Access Control List 444, 469
Assigning Privileges 457
change administrator 128, 147
File Access Definition 444, 478
initialize 128, 147
Object Association Privileges 467
Security Administrator 128
users in multiple roles 458
Optim Server 2
Access defaults 163
Archive defaults 173
Authentication 170
Choose Product Configuration File 171
Configure 151

Connection Defaults 160
default Archive directories 173
Default Directories 154
directories, limit client access to 163
Enable/Disable 132
Endpoints 169
Error defaults 156
General defaults 154
Loader defaults 158
Logon dialog 307
Maximum Processes 154
Merge Current User 159, 162
Mirror process 154
name 154, 172
Network Access 167
Personal Options 305, 306
Protocols 169
Security 171
Security defaults 166
Service Logon 165
Settings Dialog 152
Start as Process 164
Start as Service 164
Startup defaults 164
Status 177
Trace Files 155
update Configuration File 171
Oracle
create/drop packages
for DB Alias 99
for Optim Directory 85
Oracle Connection Diagnostic Tool 31

P

Password
always ask for 94
always require 101
case sensitive 142
connection information 7
credentials 417
for each workstation 10
for product options 135, 258
Product Configuration File 134
Password tab, Product Options 258
Personal Options 151–182, 279–332
actions 319
archive 315
browsing files 313
configuring 280
confirm 286
creating objects 295
database 326
DBMS loaders 293
display 287
editing data 308
email notification and configuration 330
error defaults 290
MBCS Roundtrip Processing 327
printers, language options 324
removable media 317
scheduling monitor 292
servers 268
set general defaults 284
to logon 303
PR0CMND 429
Primary Keys
creating for database 8, 233
select database tables 111
Printer Options 324–325
Processing Log
browse the log file 71
completed actions 70
Product Configuration File
additional workstations 140
configure workstations 149
creating 8
identify existing 9
set default directory 285
set default path for 257
switch configuration files 258
Product License Key
description of 7
exporting 8
for additional workstations 141
for first workstation 6
for your company 78
Product Options 245–277
archive 270

configuration file 257
configuring 246
database defaults 252
DBMS Loaders 274
editing data 259
password 258
report 276
servers 268
set general defaults 249
PST Directory Objects, converting .. 565–582
Purge
DB Alias 244
Optim Directory 243

R

README file 46
Registry Data
export file 137
from first workstation 137
importing data 142
Removable Media, Personal Options 317–318
default segment sizes 318
Replace UDTs, Personal Option 296
Report Request Editor 511–526
Email notification 522
menu commands 517
Report Type 517
Security Report 517
Report tab, Product Options 276–277
blank lines between levels 277
blank lines between rows 276
character column width 276
indent subordinate tables 277
line length 276
lines per page 276
minimum spaces between columns 277
rows per table 276
Reset Messages 289
Restore Processing
secured files 478

S

Sample
Column Map exits 599–600
Column Map procedures 601–603
Database Tables
loading 8, 112
database tables
description 588–598
structure 588
extract files 603
JCL file 603
Scheduling Monitor
directory path for 292
start immediately 293
startup options 292
Scheduling tab, Personal Options 292–293
secured files 478
Security Administrator, Optim Security 128
Security Report
creating 513
description 511
editing 515
processing 523
run 523
schedule 523
Segment
naming 318
size 317
Server Authorizations 19
Server tab, Personal Options 306–307
always ask for password 306
check logon 307
Optim Server 306
User ID, Password, Domain 306
Servers tab, Product Options 268–269
endpoint 268
network address 268
protocol 268
Server name 268
Setup
completing 46
creating desktop icons 45
customer information 39
destination folder 41
for additional workstations 9
installing application software 4

license agreement 38
program folder 44
README file 46
select components 42
type of setup 40
Special Characters
Caps mode 284
underscore as SQL LIKE 284
SQL Server
connection string 143
create multiple DB Aliases 122
create/drop procedures
for DB Alias 99
for Optim Directory 85
update DBMS version 228
Sybase ASE
connection string 143
create multiple DB Aliases 122
create shared procedures
for DB Alias 120
create/drop procedures
for DB Alias 99
for Optim Directory 85
update DBMS version 228
System Requirements
hardware/software 11
supported DBMSs 12

T

Tasks menu 183–244
access Optim Directory 191
configure additional workstations 140–150
configure first workstation 78–139
configure options 232
copy DB2 relationships 235
create additional Optim Directory 190
create primary keys 233
create/update DB Alias 96, 185–189
create/update Optim Directory 190
drop DB Alias 238–241
drop Optim Directory 238–242
enable/disable
ODBC Interface 202
Optim Server 201
load/drop sample data 236, 237
maintain access
DB Alias 205–212
Optim Directory 203–204
purge
DB Alias 244
Optim Directory 243
purpose 10
update DBMS version
for DB Alias 224–231
for Optim Directory 221–223
Trace File 284
Troubleshooting 30
Image Locator Diagnostic Tool 30
Microsoft Debugging Utility 32
Oracle Connection Diagnostic Tool 31

U

UDT 296
Uncommitted Data, Extract 254
Unicode Support 24
Uninstalling 611–614
cancel 614
do not drop all objects 614
drop all objects 613
prompt to drop all objects 613
Windows Control Panel 611
UNIX
command line 370–385
commands 391–392
customer ID 361, 372
data directories 361, 372
DB Alias 366, 375
DB Alias logon 364
destination folder 339
environment variables 386
installation 335–357
license agreement 338
loader 367, 376
locale conversion 390
LOCALE.CONF file 390
logon 364
Maximum Processes 363

Optim Directory 366, 374
permission 365
pr0pass program 399
pstlocal configuration file 370
pstserv configuration file 360
RT4S shell script 389
RTSERVER shell script 387
RTSETENV shell script 386
securing 394–402
configuration files 398–402
password file 398
select components 341
trace days 363, 373
User Defined Types
Replace UDTs, Personal Option 296
User ID
credentials 417
DB Alias access 108
Optim Directory access 93
required authority 82

W

Warn on Cascade 250, 328
Windows Registry
access to Optim Directory 7
exporting entries 8
importing entries 9
Merge Current User 10, 159, 162

Program Number:

Printed in USA